Phoenix Academy

Safeguarding & Child Protection Policy

Table of Contents

SAFEGUARDING POLICY

Incorporating our Child Protection Policy

This document has been reviewed with reference to the documents *Keeping Children Safe in Education 2021, The Prevent Duty, Departmental advice for schools and childcare providers, July 2015, Working Together to Safeguard Children 2018 and The Children Act 2004.*

This policy should be read alongside departmental advice:
What to do if you're worried a child is being abused, DfE (March 2015),
Information Sharing: Advice for practitioners, DfE (July 2018), and
non-statutory interim guidance on safeguarding in schools, colleges, and other providers.

This policy is written in line with our:

- Appointment of Staff and Safer Recruitment Policy
- Online (e-Safety) Policy
- Youth Produced Sexual Imagery (Sexting) Policy
- Preventing Extremism and Radicalisation Policy
- Whistleblowing Policy
- Behaviour Policy
- Anti-bullying Policy
- Missing Children Policy
- Staff Code of Conduct (Behaviour) Policy

These are all available on request from the school office.

SCHOOL STATEMENT

Safeguarding and promoting the welfare of children is defined for the purposes of this policy as protecting children from maltreatment; preventing impairment of children's mental and physical health or development; ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and taking action to enable all children to have the best outcomes.

The terms 'child' and 'children' includes everyone under the age of 18.

The Governors/Trustees take seriously their responsibility to protect and safeguard the welfare of children and young people entrusted to the school's care. The Governors/Trustees will ensure that persons with leadership and management responsibilities at the school demonstrate good skills and knowledge appropriate to their role and fulfil their responsibilities effectively so that the independent school standards are met consistently; and actively promote the well-being of pupils according to section 10(2) of the Children Act 2004(**a**).

Phoenix Academy is a Safeguarding School. We will invoke Child Protection Procedures where necessary.

Our Designated Safeguarding Lead is Gena Areola. Her role is to provide support and direction to staff members to carry out their safeguarding duties and to liaise closely with other services such as the local Designated Officer, the police, and the Clinical Commissioning Group(CCG), when managing referrals. As well as working closely with the principal.

Our Deputy Designated Safeguarding Lead is Paul Kelly. His role is to provide support to the Lead and be available if the Lead is unavailable.

Our Chair of Governors/Trustees is Gareth Hawkes. His role in Safeguarding is to take the lead in dealing with allegations of abuse made against the Principal/Head Teacher*.

Our Safeguarding Governor/Trustee is Gena Areola. Her role in Safeguarding is to take leadership responsibility for the school's safeguarding arrangements.

Our Principal/Head Teacher is Paul Kelly. His role in Safer Recruitment is to ensure that the school operates safe recruitment procedures and makes sure that all appropriate checks are carried out on staff and volunteers who work with the children.

Our Senior Administrator is Angela Kelly. Her role is *Insert as necessary or delete*

All staff members in the school must read the content of the policy. The *Teacher Standards 2012* states that teachers, including head teachers, should safeguard children's wellbeing and maintain public trust in the teaching profession as part of their professional duties.

All staff must undertake a regular course on safeguarding and child protection that must be updated regularly. The school is committed to an on-going training programme on such matters. Yearly updates will be undertaken at the beginning of each school year.

All staff that work directly with children must read Part 1 and Annex B "Further Information", of Keeping Children Safe in Education. Those staff not working directly with children must read either Part 1 or Annex A. The school will decide which one according to the role of the staff member. The school has systems in place to assist staff understand and discharge their role and responsibilities".

The Governors/Trustees recognise the need to build constructive links with childcare agencies, and will work with social care, the police, health services and other services to promote the welfare of children and protect them from harm.

The Governors/Trustees are committed to:

- Listening to, relating effectively and valuing children and young people whilst ensuring their protection within school activities.
- Ensuring safeguarding is taught 'as part of providing a broad and balanced curriculum', including online safety
- Employing the expertise of the staff when reviewing safeguarding policies and providing opportunities for staff to contribute to and shape safeguarding arrangements and the child protection policy.
- Encouraging and supporting parents/carers
- Ensuring that staff members are given support and training
- Ensuring all staff have an awareness of safeguarding issues that can put children at risk of harm - behaviours linked to issues such as drug taking, alcohol abuse, deliberately missing education and sexting put children in danger
- Having a system for dealing with concerns about possible abuse
- Maintaining good links with the statutory childcare authorities
- Ensuring the DSL and staff are aware of and follow local safeguarding partnership arrangements so that the school contributes to multi-agency working in line with statutory guidance, Working Together to Safeguard Children.

Where a child is suffering significant harm, or is likely to do so, action will be taken to protect that child. Action will also be taken to promote the welfare of a child in need of additional support, even if they are not suffering harm or are at immediate risk.

Everyone who encounters children, and their families has a role to play in safeguarding children. Anyone working in the school is particularly important as they are in a position to identify concerns early and provide help for children, to prevent concerns from escalating; they form part of the wider safeguarding system for children. For a description of this system, see *Working Together to Safeguard Children, 2018*.

All staff members have a responsibility to provide a safe environment in which children can learn. They have a responsibility to identify children who may be in need of extra help or who are suffering, vulnerable, or are likely to suffer, significant harm. Staff have a responsibility to review and monitor the list of these students on a regular basis and all staff members then have a responsibility to take appropriate action, working with other services as needed, including **Early Help.**

EARLY HELP

All staff should be prepared to identify children who may benefit from early help. Early help means providing support as soon as a problem emerges at any point in a child's life, from the foundation years through to the teenage years.

All staff should be aware of their local early help process and understand their role in it.

If early help is appropriate, the designated safeguarding lead (or deputy) will generally lead on liaising with other agencies and setting up an inter-agency assessment as appropriate. Staff may be required to support other agencies and professionals in an early help assessment, in some cases acting as the lead practitioner. Any such cases should be kept under constant review and consideration given to a referral to children's social care for assessment for statutory services if the child's situation does not appear to be improving or is getting worse.

Early help means providing support as soon as a problem emerges, at any point in a child's life. Providing early help is more effective in promoting the welfare of children than reacting later.

Any child may benefit from early help, but all school and college staff should be particularly alert to the potential need for early help for a child who:

- is disabled or has certain health conditions and has specific additional needs;
- has special educational needs (whether or not they have a statutory Education, Health and Care Plan);
- has a mental health need;
- is a young carer;
- is showing signs of being drawn in to anti-social or criminal behaviour, including gang involvement and association with organised crime groups or county lines;
- is frequently missing/goes missing from care or from home;
- is at risk of modern slavery, trafficking sexual or criminal exploitation;
- is at risk of being radicalised or exploited;
- has a family member in prison, or is affected by parental offending;
- is in a family circumstance presenting challenges for the child, such as drug and alcohol misuse, adult mental health issues and domestic abuse;
- is misusing drugs or alcohol themselves;
- has returned home to their family from care;
- is at risk of 'honour'-based abuse such as Female Genital Mutation or Forced Marriage;
- is a privately fostered child; and
- is persistently absent from education, including persistent absences for part of the school day.

In addition to working with the Designated Safeguarding Lead staff, staff members should be aware that they might be asked to support social workers to take decisions about individual children.

All staff members should make themselves aware of the systems within the school that support safeguarding, which are explained in the staff induction. This includes the school's safeguarding and child protection policy; the staff code of conduct; and the designated safeguarding lead.

Staff members should be aware of the signs of abuse and neglect so that they are able to identify cases of children who may be in need of help or protection. Knowing what to look for is vital to the early identification of abuse and neglect. If staff members are unsure, they should always speak to children's social care.

Staff members should be aware of any signs of extremist views of any kind in our school, whether from internal sources – students, staff or Governors/Trustees, or external sources - school community, external agencies, or individuals. Our students see our school as a safe place where they can explore controversial issues safely and where our teachers encourage and facilitate this – we have a duty to ensure this happens.

Staff members are advised to maintain an attitude of 'it could happen here' where safeguarding is concerned. When concerned about the welfare of a child, staff members should always act in the interests of the child.

A child going missing from an education setting is a potential indicator of abuse or neglect. Staff members should follow the school's procedures for dealing with children who go missing, particularly on repeat occasions. They should act to identify any risk of abuse and neglect, including sexual abuse or exploitation. More information can be found in this policy about children who run away or go missing from home or care.

If staff members have concerns about a child, they should raise these with the school's Designated Safeguarding Lead, **immediately.** This also includes situations of abuse that may involve staff members. The safeguarding lead will usually decide whether to make a referral to children's social care, although any staff member can refer their concerns to children's social care directly. Where a child and family would benefit from co-ordinated support from more than one agency (for example education, health, housing, police) an inter-agency assessment will be conducted. These assessments, undertaken by a lead professional (a teacher, special educational needs co-ordinator, General Practitioner (GP), family support worker, and/or health visitor), will identify what help the child and family require to prevent needs escalating to a point where intervention would be needed via a statutory assessment under the Children Act 1989.

A concern is when you are troubled about a child's welfare and you have reasonable cause to suspect a child is suffering, or likely to suffer, significant harm. It involves the child's safety and well-being.

If, at any point, there is a risk of immediate serious harm to a child, the DSL should be informed immediately, who will make a referral to children's social care instantly. However, anybody can make a referral in a serious situation, but please inform the DSL if you do so. If the child's situation does not appear to be improving, the staff member with concerns should press for re-consideration. Concerns should always lead to help for the child at some point.

It is important for children to receive the right help at the right time to address risks and prevent issues escalating. Research and Serious Case Reviews have repeatedly shown the dangers of failing to take effective action. Poor practice includes failing to act on and refer the

early signs of abuse and neglect, poor record keeping, failing to listen to the views of the child, failing to re-assess concerns when situations do not improve, sharing information too slowly and a lack of challenge to those who appear not to be taking action.

More information on Early Help is set out in Part one of KCSIE with full details of the early help process in Chapter one of Working Together to Safeguard Children.

CONTEXTUAL SAFEGUARDING

All staff should be aware that safeguarding incidents and/or behaviours can be associated with factors outside the school or college and/or can occur between children outside of these environments. **All** staff, but especially the designated safeguarding lead (and deputies) should consider whether children are at risk of abuse or exploitation in situations outside their families. Extra-familial harms take a variety of different forms and children can be vulnerable to multiple harms including (but not limited to) sexual exploitation, criminal exploitation, and serious youth violence.

Assessments of children should consider the wider environmental factors affecting the child's life that may pose a threat to their safety and/or welfare. As much contextual information as possible should be provided as part of the referral process. More information can be found at https://contextualsafeguarding.org.uk/

SAFER WORKING PRACTICES

The school has regard to the ***Guidance for Safer Working Practices 2015*** underpinning principles as follows:

- The welfare of the child is paramount
- Staff should understand their responsibilities to safeguard and promote the welfare of pupils
- Staff are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions
- Staff should work, and be seen to work, in an open and transparent way
- Staff should acknowledge that deliberately invented/malicious allegations are extremely rare and that all concerns should be reported and recorded
- Staff should discuss and/or take advice promptly from the headteacher if they have acted in a way which may give rise to concern
- Staff should apply the same professional standards regardless of culture, disability, gender, language, racial origin, religious belief, and sexual orientation
- Staff should not consume or be under the influence of alcohol or any substance, including prescribed medication, which may affect their ability to care for children
- Staff should be aware that breaches of the law and other professional guidelines could result in disciplinary action being taken against them, criminal action, and/or other proceedings including barring by the Disclosure & Barring Service (DBS) from working in

regulated activity, or for acts of serious misconduct prohibition from teaching by the Teaching Regulation Agency (TRA).

- Staff and managers should continually monitor and review practice to ensure this guidance is followed

- Staff should be aware of and understand their establishment's child protection policy, arrangements for managing allegations against staff, staff behaviour policy, whistle blowing procedure and their local authority safeguarding procedures.

Staff should make themselves familiar with the following school documents and policies:

- Staff Handbook

- Anti-Harassment and Bullying Policy
- Appointment of Staff Policy, incorporating Equal Opportunities in Employment Policy
- Code of Conduct Policy
- Grievance Procedure
- Management of Staff Absence Policy
- Staff Appraisal and Capability Policy
- Staff Discipline Policy
- Whistleblowing Policy
- Data Protection Policy
- Fire Safety Policy
- First Aid Policy
- Food Hygiene Policy
- Health and Safety Policy
- Risk Assessment Policy
- Anti-bullying Policy
- Behaviour Policy
- Complaints Procedure
- Confidentiality Policy
- Equal Opportunities Policy
- Exclusions Policy
- Late and Uncollected Children Policy
- Looked After Children
- Missing Child Policy
- Misuse of Substances and Drugs Policy
- Physical Interventions Policy (include the use of Reasonable Force)
- School Trips and Educational Visits Policy
- SEND Policy
- Sex and Relationship Policy
- **Online Safety**

Please refer to our Online (e-Safety) Policy. There is also a wealth of information, with links, to help schools and parents keep children safe online in KCSIE 2021 Annex D, which includes how to support keeping children safe online when they are learning at home.

KEY TRAINING AREAS

Timescale for training

Induction Training (mandatory)	Prior to starting at the school All staff, especially staff who have been redeployed in response to COVID-19, must be aware of systems within their setting which support safeguarding, and these should be explained to them as part of staff induction.
Child Protection Awareness training for whole staff including Safeguarding (statutory)	Every two years with refresher training every other year
Designated Safeguarding Lead Training (statutory)	Every two years with refresher training every other year
Safer Recruitment Training (statutory)	Every two years
Training about Preventing Terrorism (statutory)	Annually
Training for School Governors (non-statutory)	Annually
Female Genital Mutilation	Every two years
Child Sexual Exploitation	Every two years
E-Safety	Annually
Mental Health Awareness training for whole staff	TBC

IMPORTANT CONTACT DETAILS:

Safeguarding incidents could happen anywhere, and staff should be alert to possible concerns being raised in this school

Safeguarding concerns about adults in the school should be made to the Designated Safeguarding Lead or to the Head Teacher

Safeguarding concerns about independent school proprietors should go straight to the local Designated Officer - the DO.

To contact the following staff members please call the school office on: 02088876888

Gena Areola - the Designated Safeguarding Lead Person for Child Protection

Paul Kelly - the Designated Deputy Lead Person for Child Protection and Head Teacher

Gareth Hawkes – The Chair of the Trustees

Pauline Hawkes - Safer Recruitment Officer

All staff members may raise concerns directly with Children's Social Care services

The school will work with the local Designated Officer (DO) as deemed appropriate. The DO provides advice and guidance to employers and voluntary organisations that have concerns about a person working or volunteering with children and young people who may have behaved inappropriately, or you have received information that may constitute an allegation.

For further advice or help contact:

- The NSPCC Helpline: 0808 800 5000
- The NSPCC whistle-blowing helpline: 0800 028 0285

  The Police: 101 to report crime and other concerns that do not require an emergency response; 999 when there is danger to life or when violence is being used or threatened

TIMESCALES

An Initial Assessment should be initiated by the DSL or Deputy DSL within 24 hours of receipt of a referral and completed in a maximum of **10 working days**. However, this may depend on the case and the other agencies involved.

An initial assessment is deemed to be completed once the assessment has been discussed with the child and family (or caregivers) and the DSL or Deputy DSL has viewed and authorised the assessment.

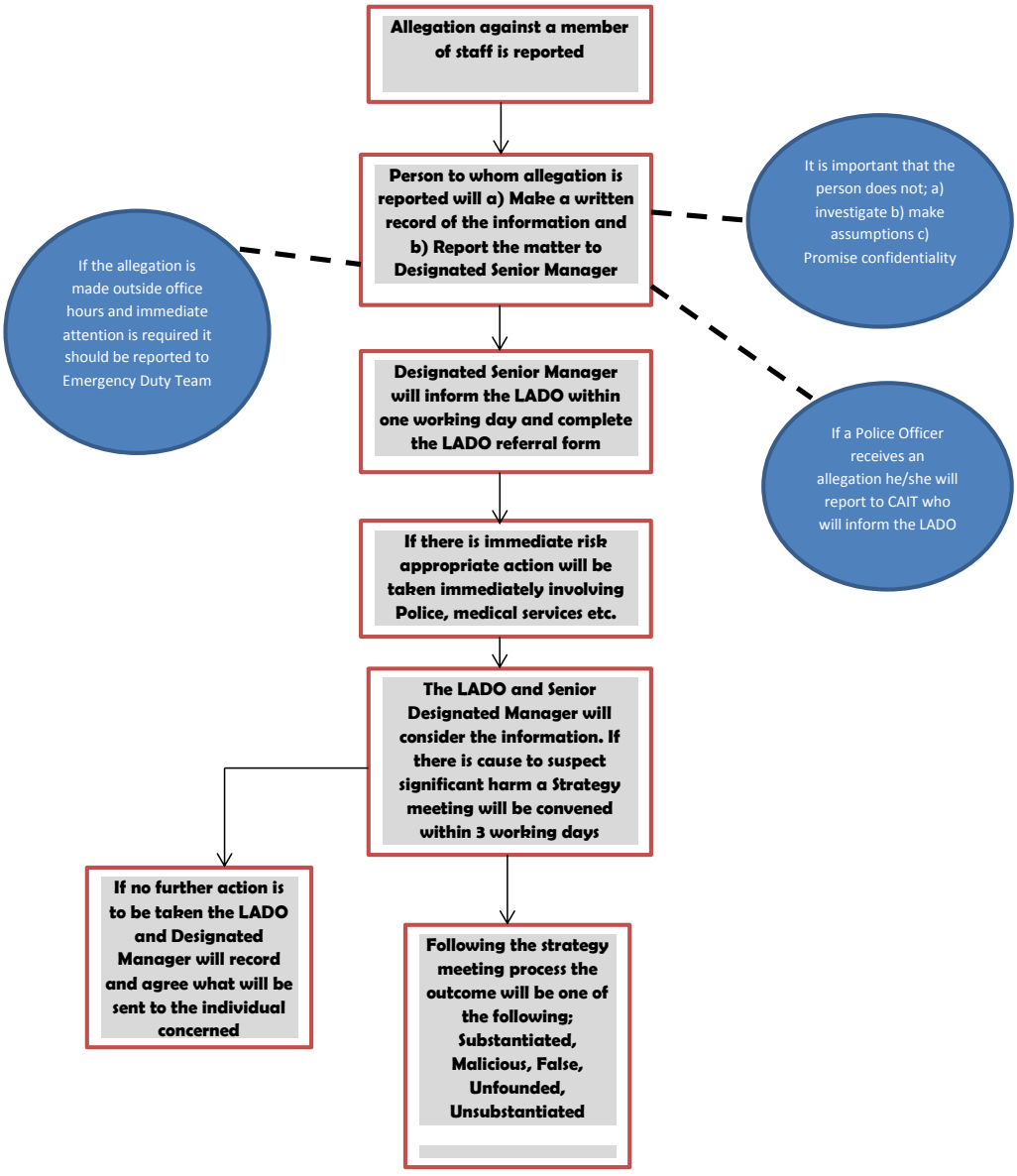
The initial assessment period may be very brief if the criteria for initiating Local Authority involvement are met, i.e., it is suspected that the child is suffering, or is likely to suffer significant harm and a strategy discussion should take place.

Any extension to timescale should be authorised by the DSL or Deputy DSL, with reasons recorded and any delay must be consistent with the welfare of the child.

See Appendix 2 for Referral Flowchart

MULTI-AGENCY LEVELS OF NEED AND RESPONSE FRAMEWORK

11. LADO REFERRAL PROCESS FLOW CHART



CHILD PROTECTION POLICY

The Governors/Trustees recognise that many children and young people today are the victims of neglect, and physical, sexual, and emotional abuse, including extremism and radicalisation. Accordingly, the Governors/Trustees have adopted the policy contained in this document, (hereafter "the policy"). The policy sets out agreed guidelines relating to the following areas:

- The Prevent Duty
- Definitions of abuse
- Responding to allegations of abuse, including those made against teachers in the school.
- Appointing teachers/assistants
- Supervision of activities and practice issues
- Helping victims of abuse
- Working with offenders
- Safer Recruitment including the level of DBS checks that will be undertaken for volunteers and Trustees

THE PREVENT DUTY

All schools and colleges are subject to a duty under section 26 of the Counterterrorism and Security Act 2015 (the CTSA 2015), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent duty.

The Prevent duty should be seen as part of schools' and colleges' wider safeguarding obligations. Designated safeguarding leads and other senior leaders in schools should familiarise themselves with the revised Prevent duty guidance: for England and Wales, especially paragraphs 57-76, which are specifically concerned with schools (and also covers childcare). Designated safeguarding leads and other senior leaders in colleges should familiar themselves with the Prevent duty guidance: for further education institutions in England and Wales. The guidance is set out in terms of four general themes: risk assessment, working in partnership, staff training, and IT policies.

Channel

Channel is a voluntary, confidential support programme which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Prevent referrals may be passed to a multi-agency Channel panel, which will discuss the individual referred to determine whether they are vulnerable to being drawn into terrorism and consider the appropriate support required. A representative from the school or college may be asked to attend the Channel panel to help with this assessment. An individual's engagement with the programme is entirely voluntary at all stages.

The designated safeguarding lead should consider if it would be appropriate to share any information with the new school or college in advance of a child leaving. For example, information that would allow the new school or college to continue supporting victims of abuse or those who are currently receiving support through the 'Channel' programme and have that support in place for when the child arrives.

Statutory guidance on Channel is available at: Channel guidance.

For additional support see page 34 KCSIE 2021

Schools providers have a critical part to play. To protect children in our care, we must be alert to any safeguarding and child protection issues in the child's life at home or elsewhere.

As a school we are expected to demonstrate activity in the following areas:

- Assessing the risk of children being drawn into terrorism.
- Demonstrate that they are protecting children and young people from being drawn into terrorism by having robust safeguarding policies.
- Ensure that their safeguarding arrangements consider the policies and procedures of the local authority, the police, and the health service.
- Make sure that staff have training that gives them the knowledge and confidence to identify children at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism
- Expected to ensure children are safe from terrorist and extremist material when accessing the internet

The school holds a separate Preventing Extremism and Radicalisation Policy with regard to this.

The full Government Prevent Strategy can be viewed at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf

The full Government Prevent Duty (2015) can be viewed at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

THE ROLE OF THE CURRICULUM *(Taken from the Preventing Extremism and Radicalisation Policy)*

We will work to ensure that our pupils will be skilled and equipped to be resilient and resist involvement in extreme or radical activities. Therefore, we recognise the need to build resilience in our pupils to make them less vulnerable.

We will therefore provide a broad and balanced curriculum within which we aim to support pupils, Spiritual, Moral, Social and Cultural development (SMSC). SMSC development is promoted through all our subjects, including the ethos of our school where development of positive attitudes and values is central to everything we do.

Values underpinning public life in the UK have been summarised as democracy, the rule of law, individual liberty, mutual respect, and the tolerance of those with different faiths and beliefs. It is important that our pupils understand this through different approaches using a balanced and broad curriculum. This supports our pupils to be responsible citizens and prepares for an adult life living and working in Britain which is diverse and changing.

Our goal is to build mutual respect and understanding and to promote the use of dialogue not violence as a form of conflict resolution. We will achieve this by using a curriculum that includes:

- Citizenship programmes
- Open discussion and debate

- Work on anti-violence and a restorative approach addressed throughout curriculum
- Focussed educational programmes

We will also work with local partners, families, and communities in our efforts to ensure our school understands and embraces our local context and values in challenging extremist views and to assist in the broadening of our pupil's experiences and horizons. We will help support students who may be vulnerable to such influences as part of our wider safeguarding responsibilities and where we believe a pupil is being directly affected by extremist materials or influences, we will ensure that that pupil is offered mentoring.

SIGNIFICANT HARM

Some children are in need because they are suffering or likely to suffer significant harm. The Children Act 1989 introduced the concept of significant harm as the threshold that justifies compulsory intervention in family life in the best interests of children. Decisions about significant harm should be informed by a careful assessment of the child's circumstances and discussion between statutory agencies and with the child and family.

INDICATORS OF ABUSE

The following definitions of child abuse are taken from the document *'Keeping Children Safe in Education'*.

Abuse

A form of maltreatment of a child. Somebody may abuse or neglect a child by inflicting harm or by failing to act to prevent harm. Children may be abused in a family or in an institutional or community setting by those known to them or, more rarely, by others. Abuse can take place wholly online, or technology may be used to facilitate offline abuse. Children may be abused by an adult or adults or by another child or children.

Physical Abuse

A form of abuse which may involve hitting, shaking, throwing, poisoning, burning, or scalding, drowning, suffocating, or otherwise causing physical harm to a child. Physical harm may also be caused when a parent or carer fabricates the symptoms of, or deliberately induces, illness in a child.

Emotional Abuse

The persistent emotional maltreatment of a child such as to cause severe and adverse effects on the child's emotional development. It may involve conveying to a child that they are worthless or unloved, inadequate, or valued only insofar as they meet the needs of another person. It may include not giving the child opportunities to express their views, deliberately silencing them or 'making fun' of what they say or how they communicate. It may feature age or developmentally inappropriate expectations being imposed on children. These may include interactions that are beyond a child's developmental capability as well as overprotection and limitation of exploration and learning or preventing the child participating in normal social interaction. It may involve seeing or hearing the ill-treatment of another. It may involve serious bullying (including cyberbullying), causing children frequently to feel frightened or in danger, or the exploitation or corruption of children. Some level of emotional abuse is involved in all types of maltreatment of a child, although it may occur alone.

Sexual Abuse

Involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving violence, whether the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing, and touching outside of

clothing. They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse. Sexual abuse can take place online, and technology can be used to facilitate offline abuse. Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children. The sexual abuse of children by other children is a specific safeguarding issue (also known as peer-on-peer abuse) in education and **all** staff should be aware of it and of their school or colleges policy and procedures for dealing with it, (see paragraph 49 KCSIE).

Neglect

The persistent failure to meet a child's basic physical and/or psychological needs, likely to result in the serious impairment of the child's health or development. Neglect may occur during pregnancy, for example, as a result of maternal substance abuse. Once a child is born, neglect may involve a parent or carer failing to: provide adequate food, clothing, and shelter (including exclusion from home or abandonment); protect a child from physical and emotional harm or danger; ensure adequate supervision (including the use of inadequate caregivers); or ensure access to appropriate medical care or treatment. It may also include neglect of, or unresponsiveness to, a child's basic emotional needs.

SPECIFIC SAFEGUARDING ISSUES

Children with special educational needs and disabilities or physical health issues

Children with special educational needs or disabilities (SEND) or certain health conditions can face additional safeguarding challenges. Additional barriers can exist when recognising abuse and neglect in this group of children. These can include:

- assumptions that indicators of possible abuse such as behaviour, mood and injury relate to the child's condition without further exploration;
- these children being more prone to peer group isolation or bullying (including prejudice-based bullying) than other children;
- the potential for children with SEND or certain medical conditions being disproportionally impacted by behaviours such as bullying, without outwardly showing any signs; and
- communication barriers and difficulties in managing or reporting these challenges.

The school will consider extra pastoral support and attention for these children, along with ensuring any appropriate support for communication is in place.

Further information can be found in the SEND Code of Practice 0 to 25 and Supporting Pupils at School with Medical Conditions.

Learners with SEN and disabilities have the following additional safeguarding vulnerabilities:

- Disabled children are at significantly greater risk of physical, sexual, and emotional abuse and neglect than non-disabled children
- Disabled children at greatest risk of abuse are those with behaviour/conduct disorders. Other high-risk groups include children with learning difficulties/disabilities, children with speech and language difficulties, children with health-related conditions and deaf children.
- Disabled children are more likely to be abused by someone in their family compared to non-disabled children. The majority of disabled children are abused by someone who is known to them.

- Bullying is a feature in the lives of many disabled children
- Disabled children are more likely to experience the negative aspects of social networking sites than non-disabled children
- Disabled children (and severely disabled children even more so) may disclose less frequently, and delay disclosure more often compared to typically developing children. Disabled children are most likely to turn to a trusted adult they know well for help such as family, friend, or teacher

Disabled children are at greater risk of abuse and significant barriers can exist to their safeguarding and wellbeing. Understanding a child's needs, building on their strengths, overcoming the barriers, and developing innovative solutions for meeting the challenges will not only enhance the child's wellbeing and protection from abuse but will provide learning that may also be of benefit for non-disabled children. Disabled children have an equal right to protection from abuse.

Child abduction and community safety incidents

Child abduction is the unauthorised removal or retention of a minor from a parent or anyone with legal responsibility for the child. Child abduction can be committed by parents or other family members; by people known but not related to the victim (such as neighbours, friends, and acquaintances); and by strangers.

Other community safety incidents in the vicinity of a school can raise concerns amongst children and parents, for example, people loitering nearby or unknown adults engaging children in conversation.

As children get older and are granted more independence (for example, as they start walking to school on their own) it is important they are given practical advice on how to keep themselves safe. Many schools provide outdoor-safety lessons run by teachers or by local police staff.

It is important that lessons focus on building children's confidence and abilities rather than simply warning them about all strangers. Further information is available at: www.actionagainstabduction.org and www.clevernevergoes.org.

Children and the Court System

Children are sometimes required to give evidence in criminal courts, either for crimes committed against them or for crimes they have witnessed. There are two age-appropriate guides to support children 5-11 year olds and 12-17 year olds.

The guides explain each step of the process, support and special measures that are available. There are diagrams illustrating the courtroom structure and the use of video links is explained.

Making child arrangements via the family courts following separation can be stressful and entrench conflict in families. This can be stressful for children. The Ministry of Justice has launched an online child arrangements information tool with clear and concise information on the dispute resolution service. This may be useful for some parents and carers.

Children Missing from Education

All staff should be aware that children going missing, particularly repeatedly, can act as a vital warning sign of a range of safeguarding possibilities. This may include abuse and neglect, which may include sexual abuse or exploitation and can also be a sign of child criminal exploitation including involvement in county lines. It may indicate mental health problems, risk of substance abuse, risk of travelling to conflict zones, risk of female genital mutilation, 'honour'-based abuse, or risk of forced marriage. Early intervention is necessary to identify the

existence of any underlying safeguarding risk and to help prevent the risks of a child going missing in future. Staff should be aware of their school's or college's unauthorised absence and children missing from education procedures.

The school has a ***Child Missing from Education*** policy, written in accordance with the *Children Missing Education Statutory Guidance for Local Authorities - September 2016, which* we will abide by concerning this area.

The school has in place appropriate safeguarding policies, procedures and responses for children who go missing from education, particularly on repeat occasions.

In the case of a child being withdrawn from the school and their whereabouts being unknown, the school will endeavour in the first place to make contact with the parents or guardians.

If no communication is received within a week, the school will contact the LEA to enquire whether they have any information regarding the child. If the LEA do not have any facts about the whereabouts of the child, we will consult with the LEA about the next step which may involve handing the case over to the local Children's Services.

If this is the case, a note will be made in the Admissions Register stating that the child's whereabouts is unknown and that they have been referred to the LEA. This will be updated if any relevant information is received.

Children with Family Members in Prison

Approximately 200,000 children in England and Wales have a parent sent to prison each year. These children are at risk of poor outcomes including poverty, stigma, isolation, and poor mental health. NICCO provides information designed to support professionals working with offenders and their children, to help mitigate negative consequences for those children.

Child Criminal Exploitation (CCE) and Child Sexual Exploitation (CSE)

We know that different forms of harm often overlap, and that perpetrators may subject children and young people to multiple forms of abuse, such as criminal exploitation (including county lines) and sexual exploitation.

In some cases, the exploitation or abuse will be in exchange for something the victim needs or wants (for example, money, gifts, or affection), and/or will be to the financial benefit or other advantage, such as increased status, of the perpetrator or facilitator.

Children can be exploited by adult males or females, as individuals or in groups. They may also be exploited by other children, who themselves may be experiencing exploitation – where this is the case, it is important that the child perpetrator is also recognised as a victim.

Whilst the age of the child may be a contributing factor for an imbalance of power, there are a range of other factors that could make a child more vulnerable to exploitation, including, sexual identity, cognitive ability, learning difficulties, communication ability, physical strength, status, and access to economic or other resources.

Some of the following can be indicators of both child criminal and sexual exploitation where children:

- appear with unexplained gifts, money, or new possessions; • associate with other children involved in exploitation;
- suffer from changes in emotional well-being;
- misuse drugs and alcohol;
- go missing for periods of time or regularly come home late; and
- regularly miss school or education or do not take part in education.

Children who have been exploited will need additional support to help maintain them in education.

CSE can be a one-off occurrence or a series of incidents over time and range from opportunistic to complex organised abuse. It can involve force and/or enticement-based methods of compliance and may, or may not, be accompanied by violence or threats of violence.

Some additional specific indicators that may be present in CSE are children who:

- have older boyfriends or girlfriends; and
- suffer from sexually transmitted infections, display sexual behaviours beyond expected sexual development or become pregnant.

Further information on signs of a child's involvement in sexual exploitation is available in Home Office guidance: Child sexual exploitation: guide for practitioners

The school holds the following document on file if ever the need arises for such information: "Child Sexual Exploitation Definition and Guide Feb 2017" and KCSIE (Annex B).

County Lines

County lines is a term used to describe gangs and organised criminal networks involved in exporting illegal drugs using dedicated mobile phone lines or other form of "deal line". This activity can happen locally as well as across the UK - no specified distance of travel is required. Children and vulnerable adults are exploited to move, store, and sell drugs and money. Offenders will often use coercion, intimidation, violence (including sexual violence) and weapons to ensure compliance of victims.

Children can be targeted and recruited into county lines in a number of locations including schools (mainstream and special), further and higher educational institutions, pupil referral units, children's homes, and care homes.

Children are also increasingly being targeted and recruited online using social media. Children can easily become trapped by this type of exploitation as county lines gangs can manufacture drug debts which need to be worked off or threaten serious violence and kidnap towards victims (and their families) if they attempt to leave the county lines network.

A number of the indicators for CSE and CCE as detailed above may be applicable to where children are involved in county lines. Some additional specific indicators that may be present where a child is criminally exploited through involvement in county lines are children who:

- go missing and are subsequently found in areas away from their home;
- have been the victim or perpetrator of serious violence (e.g., knife crime);
- are involved in receiving requests for drugs via a phone line, moving drugs, handing over and collecting money for drugs;
- are exposed to techniques such as 'plugging', where drugs are concealed internally to avoid detection;
- are found in accommodation that they have no connection with, often called a 'trap house or cuckooing' or hotel room where there is drug activity;
- owe a 'debt bond' to their exploiters;
- have their bank accounts used to facilitate drug dealing.

Further information on the signs of a child's involvement in county lines is available in guidance published by the Home Office.

Peer-on-Peer Abuse (child on child)

All staff should be aware that children can abuse other children (often referred to as peer-on-peer abuse). And that it can happen both inside and outside of school or college and online. It is important that all staff recognise the indicators and signs of peer-on-peer abuse and know how to identify it and respond to reports.

All staff should understand, that even if there are no reports in the school it does not mean it is not happening, it may be the case that it is just not being reported. As such it is important if staff have **any** concerns regarding peer-on-peer abuse, they should speak to the designated safeguarding lead (or deputy).

It is essential that **all** staff understand the importance of challenging inappropriate behaviours between peers, many of which are listed below, that are actually abusive in nature. Downplaying certain behaviours, for example dismissing sexual harassment as "just banter", "just having a laugh", "part of growing up" or "boys being boys" can lead to a culture of unacceptable behaviours, an unsafe environment for children and in worst case scenarios a culture that normalises abuse leading to children accepting it as normal and not coming forward to report it.

It is more likely that girls will be victims and boys' perpetrators, but peer-on-peer abuse is unacceptable and will be taken seriously whoever is the victim and the perpetrator.

Peer on peer abuse is most likely to include, but may not be limited to:

- bullying (including cyberbullying, prejudice-based and discriminatory bullying); abuse in intimate personal relationships between peers;
- physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm (this may include an online element which facilitates, threatens and/or encourages physical abuse);
- sexual violence, such as rape, assault by penetration and sexual assault; (this may include an online element which facilitates, threatens and/or encourages sexual violence);
- sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be standalone or part of a broader pattern of abuse;
- causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party;
- consensual and non-consensual sharing of nudes and semi-nudes images and or videos (also known as sexting or youth produced sexual imagery);
- upskirting, which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress, or alarm; and
- initiation/hazing type violence and rituals (this could include activities involving harassment, abuse or humiliation used as a way of initiating a person into a group and may also include an online element).

All staff should be clear as to the school's or college's policy and procedures with regards to peer-on-peer abuse and the important role they have to play in preventing it and responding where they believe a child may be at risk from it.

Actions the school will take

The school deals with a wide continuum of children's behaviour on a day-to-day basis and most cases will be dealt with via school-based processes. These are outlined in the following policies:

- Behaviour & Anti-Bullying Policy
- Online (e-Safety) Policy
- Attendance Policy
- Relationships and Sex Education Policy

The school will also act to minimise the risk of peer-on-peer abuse by ensuring the establishment provides a safe environment, promotes positive standards of behaviour, has effective systems in place where children can raise concerns and provides safeguarding through the curriculum via PSHE and other curriculum opportunities. This may include targeted work with children identified as vulnerable or being at risk and developing risk assessment and targeted work with those identified as being a potential risk to others.

Action on serious concerns

The school will take this issue as seriously as abuse perpetrated by an adult and address it through the same processes as any safeguarding issue. We also recognise that children who abuse others are also likely to have considerable welfare and safeguarding issues themselves.

Peer-on-peer abuse may be a one-off serious incident or an accumulation of incidents. Staff may be able to easily identify some behaviour/s as abusive however in some circumstances it may be less clear. In all cases the member of staff should discuss the concerns and seek advice from the Designated Safeguarding Lead (DSL).

When an allegation is made by a student against another student, members of staff should consider if the issues raised indicate that the child and /or alleged perpetrator may have emerging needs, complex/serious needs, or child protection concerns.

Any suspicion or allegations that a child has been sexually abused or is likely to sexually abuse another child (or adult) should be referred immediately the DSL, who will refer to the local Designated Officer (DO) or the Police, straightaway. However, staff may refer directly to the DO or police, but please inform the DSL if you do so.

All allegations should be discussed with the local Designated Officer (DO) on **the day** the allegation is made known to the school and advice sought from the DO.

Particular considerations for cases where peer on peer abuse is a factor include:

- What is the nature, extent, and context of the behaviour including verbal, physical, sexting and/or online abuse? Was there coercion, physical aggression, bullying, bribery or attempts to ensure secrecy? What was the duration and frequency? Were other children and /or adults involved?
- What is the child's age, development, capacity to understand and make decisions (including anything that might have had an impact on this i.e., coercion), and family and social circumstances?
- What are the relative chronological and developmental age of the two children and are there are any differentials in power or authority?

- Is the behaviour age appropriate or not? Does it involve inappropriate sexual knowledge or motivation?

- Are there any risks to the child themselves and others i.e., other children in school, in the child's household, extended family, peer group, or wider social network?

The school will use resources on such issues to address these matters in PSHE.

Resources on peer-on-peer pressure can be found at:
https://learning.nspcc.org.uk/research-resources/schools/resources-sexual-abuse-education-healthy-relationships

Sexual violence and sexual harassment between children in schools and colleges

All staff should be aware of indicators, which may signal that a child is at risk from or is involved with serious violent crime. These may include increased absence from school, a change in friendships or relationships with older individuals or groups, a significant decline in performance, signs of self-harm or a significant change in wellbeing, or signs of assault or unexplained injuries. Unexplained gifts or new possessions could also indicate that children have been approached by, or are involved with, individuals associated with criminal networks or gangs.

All staff should be aware of the associated risks and understand the measures in place to manage these. Advice for schools and colleges is provided in the Home Office's Preventing youth violence and gang involvement and its Criminal exploitation of children and vulnerable adults: county lines guidance.

Sexual violence and sexual harassment can occur between two children of any age and sex from primary to secondary stage and into colleges. It can also occur online. It can also occur through a group of children sexually assaulting or sexually harassing a single child or group of children.

Children who are victims of sexual violence and sexual harassment will likely find the experience stressful and distressing. This will, in all likelihood, adversely affect their educational attainment and will be exacerbated if the alleged perpetrator(s) attends the same school or college. Sexual violence and sexual harassment exist on a continuum and may overlap, they can occur online and face to face (both physically and verbally) and are never acceptable.

It is essential that **all** victims are reassured that they are being taken seriously and that they will be supported and kept safe. A victim should never be given the impression that they are creating a problem by reporting sexual violence or sexual harassment. Nor should a victim ever be made to feel ashamed for making a report.

Staff should be aware that some groups are potentially more at risk. Evidence shows girls, children with special educational needs and disabilities (SEND) and LGBT children are at greater risk.

Staff should be aware of the importance of:

- challenging inappropriate behaviours;

- making clear that sexual violence and sexual harassment is not acceptable, will never be tolerated and is not an inevitable part of growing up;

- not tolerating or dismissing sexual violence or sexual harassment as "banter", "part of growing up", "just having a laugh" or "boys being boys"; and,

- challenging physical behaviours (potentially criminal in nature), such as grabbing bottoms, breasts and genitalia, pulling down trousers, flicking bras and lifting up skirts. Dismissing or tolerating such behaviours risks normalising them.

Sexual Violence

It is important that school staff are aware of sexual violence and the fact children can, and sometimes do, abuse their peers in this way and that it can happen both inside and outside of school. When referring to sexual violence we are referring to sexual offences under the Sexual Offences Act 2003 as described below:

Rape: A person (A) commits an offence of rape if: he intentionally penetrates the vagina, anus, or mouth of another person (B) with his penis, B does not consent to the penetration and A does not reasonably believe that B consents.

Assault by Penetration: A person (A) commits an offence if: s/he intentionally penetrates the vagina or anus of another person (B) with a part of her/his body or anything else, the penetration is sexual, B does not consent to the penetration and A does not reasonably believe that B consents.

Sexual Assault: A person (A) commits an offence of sexual assault if: s/he intentionally touches another person (B), the touching is sexual, B does not consent to the touching and A does not reasonably believe that B consents. Staff should be aware that sexual assault covers a very wide range of behaviour so a single act of kissing someone without consent or touching someone's bottom/breasts/genitalia without consent, can still constitute sexual assault.

Causing someone to engage in sexual activity without consent: A person (A) commits an offence if: s/he intentionally causes another person (B) to engage in an activity, the activity is sexual, B does not consent to engaging in the activity, and A does not reasonably believe that B consents. (This could include forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party.)

For information on 'What is consent' see page 137 KCSIE 2021

Sexual Harassment

Sexual harassment is 'unwanted conduct of a sexual nature' that can occur online and offline and both inside and outside of school. When we reference sexual harassment, we do so in the context of child-on-child sexual harassment. Sexual harassment is likely to: violate a child's dignity, and/or make them feel intimidated, degraded, or humiliated and/or create a hostile, offensive or sexualised environment.

Whilst not intended to be an exhaustive list, sexual harassment can include:

- sexual comments, such as: telling sexual stories, making lewd comments, making sexual remarks about clothes and appearance, and calling someone sexualised names;

- sexual "jokes" or taunting;

- physical behaviour, such as: deliberately brushing against someone, interfering with someone's clothes (the school will consider when any of this crosses a line into sexual violence - it is important to talk to and consider the experience of the victim) and displaying pictures, photos, or drawings of a sexual nature; and

- online sexual harassment. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:

- non-consensual sharing of nudes and semi-nudes images and/or videos; As set out in UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people (which provides detailed advice for schools and colleges) taking and sharing nude photographs of U18s is a criminal offence;
    - sharing of unwanted explicit content;
    - upskirting (is a criminal offence141);
    - sexualised online bullying;
    - unwanted sexual comments and messages, including, on social media; and
    - sexual exploitation; coercion and threats

Robust guidance on this matter may be found in Keeping Children Safe in Education Part 5, and in the DfE guidance *Sexual Violence and Sexual Harassment between Children in Schools and Colleges.* This document covers:

- What sexual violence and harassment is
- Schools' and colleges' legal responsibilities
- A whole school or college approach to safeguarding and child protection
- How to respond to reports of sexual violence and sexual harassment

Female Genital Mutilation

Female Genital Mutilation (FGM) comprises all procedures involving partial or total removal of the external female genitalia or other injury to the female genital organs. It is illegal in the UK and a form of child abuse with long-lasting harmful consequences.

Teachers have **a specific legal duty to act** with regards to concerns about female genital mutilation (FGM) and must personally report to the police a disclosure that FGM has been carried out (in addition to liaising with the DSL). However, all staff should also speak to the DSL where there are concerns.

The school will access the following documents if ever the need arises for such information, as referred to in Annex B of KCSIE 2021:
'FGM mandatory reporting duty for teachers' KCSIE 2021 page 131
'Multi-Agency Statutory Guidance on Female Genital Mutilation'
'FGM Resource Pack'
'FGM Fact Sheet'

Mental Health

All staff should be aware that mental health problems can, in some cases, be an indicator that a child has suffered or is at risk of suffering abuse, neglect or exploitation.

Only appropriately trained professionals should attempt to make a diagnosis of a mental health problem. Education staff however, are well placed to observe children day-to-day and identify those whose behaviour suggests that they may be experiencing a mental health problem or be at risk of developing one.

Where children have suffered abuse and neglect, or other potentially traumatic adverse childhood experiences, this can have a lasting impact throughout childhood, adolescence and into adulthood. It is key that staff are aware of how these children's experiences, can impact on their mental health, behaviour, and education.

If staff have a mental health concern about a child that is also a safeguarding concern, immediate action should be taken, following their child protection policy, and speaking to the designated safeguarding lead or a deputy.

See KCSIE 2021, paragraph 44 for advice and guidance on *Mental Health and Behaviour in Schools*, and links to other resources.

Preventing Radicalisation

Children are vulnerable to extremist ideology and radicalisation. Similar to protecting children from other forms of harms and abuse, protecting children from this risk should be a part of a schools' or colleges' safeguarding approach.

- **Extremism** is the vocal or active opposition to our fundamental values, including democracy, the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs. This also includes calling for the death of members of the armed forces.
- **Radicalisation** refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.
- **Terrorism** is an action that endangers or causes serious violence to a person/people; causes serious damage to property; or seriously interferes or disrupts an electronic system. The use or threat **must** be designed to influence the government or to intimidate the public and is made for the purpose of advancing a political, religious, or ideological cause.

There is no single way of identifying whether a child is likely to be susceptible to an extremist ideology. Background factors combined with specific influences such as family and friends may contribute to a child's vulnerability. Similarly, radicalisation can occur through many different methods (such as social media or the internet) and settings (such as within the home).

However, it is possible to protect vulnerable people from extremist ideology and intervene to prevent those at risk of radicalisation being radicalised. As with other safeguarding risks, staff should be alert to changes in children's behaviour, which could indicate that they may be in need of help or protection. Staff should use their judgement in identifying children who might be at risk of radicalisation and act proportionately which may include the designated safeguarding lead (or deputy) making a Prevent referral.

So-called 'honour'-based abuse (including Female Genital Mutilation and Forced Marriage)

So-called 'honour'-based abuse (HBA) encompasses incidents or crimes which have been committed to protect or defend the honour of the family and/or the community, including female genital mutilation (FGM), forced marriage, and practices such as breast ironing. Abuse committed in the context of preserving 'honour' often involves a wider network of family or community pressure and can include multiple perpetrators. It is important to be aware of this dynamic and additional risk factors when deciding what form of safeguarding action to take. All forms of HBA are abuse (regardless of the motivation) and should be handled and escalated as such. Professionals in all agencies, and individuals and groups in relevant communities, need to be alert to the possibility of a child being at risk of HBA, or already having suffered HBA.

Actions

If staff have a concern regarding a child who might be at risk of HBA or who has suffered from HBA, they should speak to the designated safeguarding lead (or deputy). As appropriate, the designated safeguarding lead (or deputy) will activate local safeguarding procedures, using existing national and local protocols for multi-agency liaison with police and children's social

care. Where FGM has taken place, since 31 October 2015 there has been a mandatory reporting duty placed on **teachers** that requires a different approach (see section on FGM).

Further information may be found in the following guidance:

- FGM - page 31 KCSIE 2021
- Forced marriage – page 32 KCSIE 2021
- Female genital mutilation: information and resources- Home Office guidance
- Female genital mutilation: multi agency statutory guidance - DfE, DH, and HO statutory guidance
- Forced marriage - Forced Marriage Unit (FMU) statutory guidance
- FGM resource pack – HM Government guidance

OTHER SAFEGUARDING ISSUES

Specific Issues

Staff need to be aware of the following specific issues. The school holds policies on those marked with an *

Guidance and practical support on these specific safeguarding issues will be sought form expert and professional organisations, if and when needed, using the NSPCC and GOV.UK websites. Links to **Additional Advice and Support** may be found on pages 140-142 of KCSIE 2021, which signpost schools towards further information on specific safeguarding issues.

- Modern Slavery and the National Referral Mechanism *(KCSIE 2021 page 127)*
- Cybercrime *(KCSIE 2021 page 127)*
- Domestic Abuse – inc. 'teenage relationship abuse' *(KCSIE 2021 page 128-129)*

  Additional advice on identifying children who are affected by domestic abuse and how they can be helped is available at:

  - NSPCC- UK domestic-abuse Signs Symptoms Effects
  - Refuge what is domestic violence/effects of domestic violence on children
  - Safelives: young people and domestic abuse.
  - Domestic abuse: specialist sources of support - GOV.UK (www.gov.uk) (includes information for adult victims, young people facing abuse in their own relationships and parents experiencing child to parent violence/abuse)
- Bullying including cyberbullying - see our 'Online (e-Safety) Policy'
- Children requiring mental health support (See KCSIE 2021, page 42)
- Children who need a social worker (Child in Need and Child Protection Plans) (See KCSIE 2021, page 41)
- Drugs*
- Fabricated or induced illness
- Faith based abuse
- Forced marriage

- Gangs and youth violence
- Hate – see Educate Against Hate and Appendix I of our Anti-Bullying Policy
- Homelessness – the DSL should be aware of the contact details and referral routes of the Local Housing Authority to enable them to raise concerns. Referrals to the Local Housing Authority should not replace referrals to children's social care where a child is being harmed or at risk of harm. Schools should recognise that for 16- and 17-year-olds homelessness may not be family-based, and the DSL should ensure appropriate referrals to children's services are made where necessary. (See KCSIE 2021 page 130).
- Looked after children and previously looked after children (See KCSIE 2021 page 44)
- Private fostering (See KCSIE 2021 page 77)
- Sexting / Sharing nudes and semi-nudes – See The UK Council for Internet Safety (UKCIS) non-statutory guidance on Youth Produced Sexual Imagery (YPSI), entitled '**Sharing nudes and semi-nudes: advice for education settings working with children and young people**' and our 'Sharing nudes and semi-nudes Policy'

Alternative Provision

- If the school places a pupil with an alternative provision provider, they remain responsible for the safeguarding of that pupil and should be satisfied that the provider meets the needs of the pupil. The provider should provide written confirmation that appropriate safeguarding checks have been carried out on those working at the establishment.

Adults Who Supervise Children on Work Experience

- When organising work placements, the school will ensure that the placement provider has policies and procedures in place to safeguard pupils.

Children staying with Host Families (Homestay) – *See Annex E KCSIE*

Sharing Safeguarding/Child Protection Information with a New School or College

When a pupil with child protection issues moves school, the DSL should consider whether it is appropriate to share any information with the new school or college in advance of a pupil leaving, in addition to the child protection file. The DfE gives the example of information that would allow the new school or college to continue supporting a victim of abuse and have the appropriate support in place for the pupil's arrival.

RECOGNISING AND RESPONDING TO ABUSE

The following signs may or may not be indications that abuse has taken place, but the possibility should be considered.

Physical Signs of Abuse

- Any injuries not consistent with the explanation given for them.
- Injuries that occur to the body in places that are not normally exposed to falls, rough games, etc.
- Injuries which have not received medical attention
- Neglect – under nourishment, failure to grow, constant hunger, stealing or gorging food, untreated illnesses, inadequate care, etc.
- Reluctance to change for, or participate in games or swimming
- Repeated urinary infections or unexplained tummy pains
- Bruises, bites, burns, fractures etc., which do not have an accidental explanation
- Cuts/ scratches/ substance abuse

Indicators of Possible Sexual Abuse

- Any allegations made by a child concerning sexual abuse
- Any allegations made by a child concerning female genital mutation
- Child with excessive preoccupation with sexual matters and detailed knowledge of adult sexual behaviour, or who regularly engages in age-inappropriate sexual play
- Sexual activity through words, play or drawing
- Child who is sexually provocative or seductive with adults
- Inappropriate bed-sharing arrangements at home
- Severe sleep disturbances with fears, phobias, vivid dreams, or nightmares, sometimes with overt or veiled sexual connotations
- Eating disorders – anorexia, bulimia

Emotional Signs of Abuse

- Changes or regression in mood or behaviour, particularly where a child withdraws or becomes clinging. Also, depression/ aggression, extreme anxiety
- Nervousness, frozen watchfulness
- Obsessions or phobias
- Sudden under-achievement or lack of concentration
- Inappropriate relationships with peers and/ or adults

- Attention-seeking behaviour
- Persistent tiredness
- Running away/ stealing/ lying

WHAT TO DO IF YOU SUSPECT THAT ABUSE MAY HAVE OCCURRED

1 You must report concerns as soon as possible to Gena Areola, the Designated Safeguarding Officer (DSL), who is nominated by the Governors/Trustees to act on their behalf in referring allegations or suspicions of neglect or abuse to the statutory authorities. She may also be required by conditions of the School Insurance Policy to immediately inform the Insurance Company. In the absence of the DSL, the matter should be brought to the attention of Paul Kelly (hereafter the "Deputy DSL"). In all instances telephone 02088876888.

If the suspicions in any way involve the DSL or Deputy DSL, then the report should be made to the Safeguarding Governor who should contact the local Designated Officer (DO).

2 Staff should only involve those who need to be involved when a child tells them he/she is being abused or neglected. Suspicions will not be discussed with anyone other than those nominated above

3 Although members of the school are expected to use the procedure stated in step 1, it is, of course, the right of any individual as a citizen to make direct referrals to the child protection agencies or seek advice from a reputable safeguarding agency. Please inform the DSL immediately, if you do so. If, however, you feel that the DSL or Deputy DSL have not responded appropriately to your concerns, then it is open to you to contact the relevant organisation direct. We hope that by making this statement that we demonstrate the commitment of the school to effective child protection.

ALLEGATIONS OF PHYSICAL INJURY OR NEGLECT

If a child has a physical injury or symptom of neglect, the DSL will:

1 Contact the local Designated Officer (DO) for advice in cases of deliberate injury or when concerned about the child's safety. The school in these circumstances should not inform the parents.

2 Where emergency medical attention is necessary it will be sought immediately. The DSL will inform the doctor of any suspicions of abuse.

3 In other circumstances speak with the parent/ carer and suggest that medical help/ attention be sought for the child. The doctor (or health visitor) will then initiate further action, if necessary.

4 If appropriate, the parent/ carer will be encouraged to seek help from the Local Authority.

5 Where the parent/ carer is unwilling to seek help, if appropriate, the DSL will offer to go with them. If they still fail to act, the DSL should, in cases of real concern, contact the local Safeguarding Children Partnership for advice.

ALLEGATIONS OF SEXUAL ABUSE

In the event of allegations or suspicions of sexual abuse, the DSL will:

Contact the Police Child Protection Team directly. The DSL will NOT speak to the parent (or anyone else).

1 If, for any reason, the DSL is unsure whether or not to follow the above, then advice from the local Designated Officer (DO) will be sought and followed.

2 Under no circumstances will the DSL attempt to carry out any investigation into the allegation or suspicions of sexual abuse. The role of the DSL is to collect and clarify the precise details of the allegation or suspicion and to provide this information to the DO, whose task it is to investigate the matter under Section 47 of the Children Act 1989

3 Whilst allegations or suspicions of sexual abuse will normally be reported to the DSL, the absence of the DSL or Deputy DSL should not delay referral to the DO

4 Exceptionally, should there be any disagreement between the person in receipt of the allegation or suspicion and the DSL or Deputy DSL as to the appropriateness of a referral to the DO, that person retains a responsibility as a member of the public to report serious matters to the DO, and should do so without hesitation

5 The Governors/Trustees will support the DSL or Deputy DSL in their role and accept that any information they may have in their possession will be shared in a strictly limited way on a need to know basis.

HOW TO RESPOND TO A CHILD WANTING TO TALK ABOUT ABUSE

It is not easy to give precise guidance, but the following may help:

General Points

- Show acceptance of what the child says (however unlikely the story may sound)
- Keep calm
- Look at the child directly
- Be honest
- Tell the child you will need to let someone else know – don't promise confidentiality
- Even when a child has broken a rule, they are not to blame for the abuse
- Be aware that the child may have been threatened or bribed not to tell
- Never push for information. If the child decides not to tell you after all, then accept that and let them know that you are always ready to listen

Helpful things you may say or show

- "I believe you"
- Show acceptance of what the child says
- "Thank you for telling me"

- "It's not your fault"
- "I will help you"

Do not say

- "Why didn't you tell anyone before"
- "I can't believe it!"
- "Are you sure this is true?"
- "Why? How? When? Who? Where?"
- Never make false promises
- Never make statements such as "I am shocked, don't tell anyone else"

Concluding

- Again, reassure the child what you are going to do next and that you will let them know what happens (the DSL might have to consider referring to the Children, Schools and Families department or the Police to prevent a child or young person returning home if the school considers them to be seriously at risk of further abuse)
- Contact the person in the school responsible for coordinating child protection concerns or contact the Children, Schools and Families department / Police/ NSPCC
- Consider your own feelings and seek pastoral support if needed

WHAT TO DO ONCE A CHILD HAS TALKED TO YOU ABOUT ABUSE

The Procedure

- Make notes as soon as possible (preferably within one hour of the child talking to you), writing down exactly what the child said and when she/he said it, what you said in reply and what was happening immediately beforehand (e.g., a description of the activity). Record dates and times of these events and when you made the record. Keep all hand-written notes, even if subsequently typed. Such records should be kept safely for an indefinite period.

  Use the form "Responding to abuse – worker's action sheet"

- Report your discussion as soon as possible to the DSL. If the latter is implicated report to the Deputy DSL. If all are implicated, report to the Safeguarding Governor, who should contact the local Designated Officer (DO).
- You should not discuss your suspicions or allegations with anyone other than those nominated in the above point.
- Once a child has talked about abuse the DSL should consider whether it is safe for a child to return home to a potentially abusive situation. On rare occasions, it might be necessary to take immediate action to contact the DO and/ or Police to discuss putting into effect safety measures for the child so that they do not return home.

WORKING WITH OFFENDERS

The Governors/Trustees in their commitment to the protection of all children will meet with the individual and discuss boundaries that the person will be expected to keep.

Offenders will be expected to sign a contract stipulating boundaries and will involve the person's family and partner who will need to be informed.

HELPING VICTIMS OF ABUSE – THE CHILD'S WISHES

As a Christian school, we are committed to supporting victims of abuse, and encouraging them in their faith.

The school will ensure the child's wishes or feelings are considered when determining what action to take and what services to provide to protect individual children through ensuring there are systems in place for children to express their views and give feedback. Staff members should not promise confidentiality to the child and always act in the **best interests** of the child.

ARRANGEMENTS FOR SUPERVISION OF GROUP/ CHILDREN'S ACTIVITIES

Practical Issues

- A register of children or young people attending the activity should be kept, and a register of helpers.
- A log of each activity, recording any unusual events with each teacher/assistant recording what they witnessed should be kept.
- Incidents such as fights and what action the teacher/assistant took should be recorded in the logbook.
- Accidents and injuries should be recorded in a separate accident book and parents and older children should be asked to sign this.
- No person under 16 years of age should be left in charge of any children of any age. Nor should children or young people attending school be left alone at any time.

Boundaries

- All staff members should treat all children/young people with dignity and respect in attitude, language used and actions.
- Respect the privacy of children, avoid questionable activity.
- If you invite a child to your home, ensure this is with the knowledge of the Head Teacher / Principal and that a parent is aware.
- Ensure that all transport arrangements have parental approval and are with the knowledge of the leadership.
- Only staff members assigned to a group should be allowed into rooms. Other adults should not have free access. Ensure you note anybody else who is there for a specific reason in the logbook.

OFF-SITE VISITS

Appropriate risk assessments must be in place prior to any off-site visit taking place.

Any overnight visit will explicitly set out sleeping arrangements; the role and responsibility of each adult, whether employed or volunteers; on/off duty arrangements; clear expectations about boundaries and interactions with children/young people; and expectations around smoking/drinking by adult.

Safeguarding concerns or allegations will be responded to following the school safe-guarding procedures. The member of staff in charge of the visit will report any safeguarding concerns to the Designated Safeguarding Lead and Head teacher/Principal, who will pass to the local Designated Officer (DO) if appropriate. In an emergency, the staff member in charge will contact the police and/or social care.

POLICY ON SUSPICIONS OR ALLEGATIONS OF CHILD ABUSE INVOLVING SCHOOL STAFF

Staff, including volunteers, must be aware that they may be vulnerable to accusations of abuse and must, therefore, be sensitive to a child's reaction to physical contact and react appropriately. During their daily contact with the children, all staff must be aware of the following:

- It is the policy of Name of School not to kiss the pupils.
- Staff should not touch a child in such a way or on parts of the body that might be considered indecent.
- Staff should avoid restraining children, except under certain circumstances when it is unavoidable (See Policy on Restraint).
- Staff should maintain professional standards of behaviour and appropriate boundaries at all times in relationships between themselves and the pupils, themselves, and the parents.
- A member of staff, who feels that they may be at risk of being accused of behaving inappropriately, should request the presence of another member of staff.
- No form of corporal punishment should ever be used, nor its use ever threatened.
- When it is necessary to restrain a child to prevent injury to themselves, others, or property, only the minimum force should be used and injury to the child concerned should be avoided. Any arm or hands should never be placed around a child's neck.

If there is an allegation or suspicion of misconduct about a member of staff, the Principal/Head Teacher* must be informed immediately. Failure to do so may result in disciplinary action

If the allegation or suspicion in any way involves the DSL or Deputy DSL, then the report should be made to the Safeguarding Governor, 02088876888 who should contact the local Designated Officer (DO) on _(Tel. no.) 020 8379 5555 or email **TheMashTeam@enfield.gov.uk** and give as much information as you can.

The school is required to inform the Disclosure and Barring Service as soon as investigations are completed, any person, whether employed, contracted, a volunteer, or a student, whose services are no longer used because he or she is considered unsuitable to work with children.

The address for referrals is DBS customer services, PO Box 3961, Royal Wootton Bassett SN4 4HF - Telephone 03000 200 190. Failure by the school to make such a report could constitute an offence, leading to the school being removed from the DfE's register of Independent Schools (legislation from The Education (Provision of Information by

Independent Schools) (England) Regulations 2003. Compromise Agreements cannot apply in this connection.

The school will also make a referral to the Disclosure and Barring Service (DBS) if a person in regulated activity has been dismissed or removed due to safeguarding concerns or would have been had they not resigned.

Schools and colleges have a legal duty to refer to the DBS anyone who has harmed, or poses a risk of harm, to a child or vulnerable adult where:

- the harm test is satisfied in respect of that individual;
- the individual has received a caution or conviction for a relevant offence, or if there is reason to believe that the individual has committed a listed relevant offence; and
- the individual has been removed from working (paid or unpaid) in regulated activity or would have been removed had they not left.

A person satisfies the harm test if they may harm a child or vulnerable adult or put them at risk of harm. It is something a person may do to cause harm or pose a risk of harm to a child or vulnerable adult. (*See https://www.gov.uk/guidance/making-barring-referrals-to-the-dbs#what-is-the-harm-test).*

The Teaching Regulation Agency (TRA) will also be informed if staff are sacked due to safeguarding issues https://teacherservices.education.gov.uk/

Regard must be given to the section 'Allegations of Abuse Made Against Teachers and Other Staff', in the document 'Keeping Children Safe in Education', which is on file in the school office. This should be used in respect of all cases in which it is alleged that a teacher or member of staff (including supply staff and volunteers) in a school or college that provides education for children under 18 years of age has:

- Behaved in a way that has harmed a child, or may have harmed a child;
- Possibly committed a criminal offence against or related to a child; or
- Behaved towards a child or children in a way that indicates he or she **may** pose a risk of harm to children.
- Behaved or may have behaved in a way that indicates he or she may not be suitable to work with children.

This is due to the principle of transferrable risk where an individual is involved in an incident outside of school which did not involve children but could have an impact on their suitability to work with children. For example, domestic violence at home – even if no children were involved, could a child trigger the same reaction, and thereby be put at risk.

ALLEGATIONS AGAINST PUPILS

The School's policies on behaviour, bullying, discipline and sanctions should be read in conjunction with this policy and will also apply to this situation. Bullying should be treated as a child protection concern when there is reasonable cause to suspect that a child is suffering or likely to suffer significant harm. A pupil against whom an allegation of abuse has been made may be suspended from the School during the investigation if it is considered to be in the interests of a child who might otherwise be at risk, in the interests of the pupils at large or to allow the investigation to proceed more effectively.

POLICY FOR CHILDREN LOOKED AFTER

The school recognises that children looked after/ children in care are one of the most vulnerable groups of children so need more frequent observational assessment to meet their needs. All staff will be made aware of anyone in the school who is looked after so that the child can be supported adequately. On admission, it will be established who has parental responsibility so that statutory requirements are met.

The Governing body will ensure that staff have the skills, knowledge and understanding to keep looked after children or previously looked after children safe. Appropriate staff will have the information they need in relation to a child's looked after legal status (whether they are looked after under voluntary arrangements with consent of parents or on an interim or full care order) and contact arrangements with birth parents or those with parental responsibility. Information about the child's care arrangements and the levels of authority delegated to the carer by the authority looking after him/her will be available for all staff involved, including the designated safeguarding lead having details of the child's social worker.

When dealing with looked after children and previously looked after children, the school will work together with all agencies involved and take prompt action when necessary to safeguard these children, who are a particularly vulnerable group.

The school holds a policy for Children Looked After on file.

CARE LEAVERS

*A **care leaver** is defined as a person aged 25 or under, who has been looked after by a local authority for at least 13 weeks since the age of 14; and who was looked after by the local authority at school-leaving age or after that date.*

If the need arises, the Designated Safeguarding Lead will liaise as necessary with the local authority Personal Advisor appointed to guide and support the care leaver, regarding any issues of concern affecting the care leaver.

PHYSICAL INTERVENTION POLICY AND USE OF REASONABLE FORCE

The school holds a Physical Intervention Policy, which includes the use of reasonable force

PHOTOGRAPHY AND IMAGES The following is an example that you could use or change to your own policy

To protect children, we will:

- Seek parental consent for photographs to be taken or published (for example, on our website or in newspapers or publications)
- Only use school equipment
- Only take photos and videos of children to celebrate achievement
- Use only the child's first name with an image
- Ensure that children are appropriately dressed
- Encourage children to tell us if they are worried about any photographs that are taken of them.

The school will issue a statement that where parents are taking photographs of children related to school events these are to be for personal use only (these are not to be shared on social media for example).

EXTERNAL VISITORS/CONTRIBUTORS/SPEAKERS

Visitors with a professional role, such as the school nurse, social worker, educational psychologist, or members of the Police will have had the appropriate vetting checks undertaken by their own organisation. Any professionals visiting the school should provide evidence of their professional role and employment details (an identity badge for example). If felt necessary, the school will contact the relevant organisation to verify the individual's identity.

The school has a separate policy for visiting speakers

AGENCY STAFF

The school will check that any agency staff member attending the school is the same person that the agency has provided the vetting checks for.

If staff supplied by an employment business have lived outside the UK, the employment business must have made additional checks for the appropriate countries, and the school will get written confirmation to that effect from the employment business.

SAFER RECRUITMENT

The school will follow the procedures as laid out in the school's 'Appointment of Staff and Safer Recruitment Policy'. A brief summary follows.

- Before employing a teacher, the school will take all reasonable steps to establish whether the individual is subject to a teacher prohibition order and, if so, prevent their employment.

- The school will verify a candidate's identity, preferably from current photographic ID and proof of address except where, for exceptional reasons, none is available.

- Enhanced DBS checks will be undertaken for all staff, including volunteers who are carrying out relevant, unsupervised activities with the students, and all Governors/Trustees. When responding to questions from the school about their criminal record, staff do not need to provide details about any protected cautions or protected convictions.

- Those in regulated activity will need an enhanced DBS certificate with barred list check *(See point 26).* A **supervised** volunteer who regularly teaches or looks after children **is not in regulated activity**.

- A separate barred list check (List 99 check) will be obtained if an individual will start work in regulated activity before the DBS certificate is available

- A Prohibition from Teaching Check will be completed for *everyone* engaged in 'teaching work', *(see point 27)* whether a qualified teacher or not; and recorded on the Single Central Record, to ensure they are not prohibited from teaching, using **Teacher Services** (https://www.gov.uk/guidance/teacher-status-checks-information-for-employers).

  Even people with QTS, MUST have this prohibition check entered into the Single Central Record. The Teacher Service's system will be used to verify any award of QTS and the completion of an induction/probation.

- All leaders and managers, including Trustees/Governors are now required to have a **section 128 Management Check –** This will be included on the school's SCR showing that checks have been according to section 128. This will also be done using Teacher Services (as point 7).

  Note: Section 128 directions will show on an enhanced DBS check with barred list information, provided that '**children's workforce independent schools**' is specified in the parameters of the check.

- Individuals who have lived or worked outside the UK must undergo the same checks as all other staff in schools or colleges. *See paragraphs 262 -267 KCSIE 2021*. This includes obtaining (via the applicant) an enhanced DBS certificate (including barred list information, for those who will be engaging in regulated activity) even if the individual has never been to the UK. In addition, the school will make any further checks they think appropriate so that any relevant events that occurred outside the UK can be considered. These checks could include, where available:
  - criminal records checks for overseas applicants - Home Office guidance can be found on GOV.UK; and for teaching positions
  - obtaining a letter (via the applicant) from the professional regulating authority in the country (or countries) in which the applicant has worked confirming that they have not imposed any sanctions or restrictions, and or that they are aware of any reason why they may be unsuitable to teach[87]. Applicants can find

contact details of regulatory bodies in the EU/EEA and Switzerland on the Regulated Professions database. Applicants can also contact the UK Centre for Professional Qualifications who will signpost them to the appropriate EEA regulatory body.

Where available, such evidence can be considered together with information obtained through other pre-appointment checks to help assess their suitability. Where this information is not available the school will seek alternative methods of checking suitability and or undertake a risk assessment that supports informed decision making on whether to proceed with the appointment. Although sanctions and restrictions imposed by another regulating authority do not prevent a person from taking up teaching positions in England, the school will consider the circumstances that led to the restriction or sanction being imposed when considering a candidate's suitability for employment. *Further information can be found in DfE Guidance: Recruit teachers from overseas.* All steps taken will be well documented.

- Applicants will be asked to supply a declaration of their mental and physical fitness to carry out their work responsibilities. A job applicant can be asked relevant questions about disability and health in order to establish whether they have the physical and mental capacity for the specific role.

- The applicant's right to work in the UK will be checked and evidence kept on record.

- As part of our Safeguarding Policy employment will not be offered without the applicant supplying evidence of a full employment history, including information on any gaps.

- Two professional references will be requested, for all staff, including volunteers, which go back 5 years, from senior persons and not just colleagues; character and/or pastoral references will only be requested where appropriate or relevant. Where possible, references will be obtained prior to interviews to allow any concerns to be explored with the referee and discussed with the candidate.

The criteria for NOT appointing children's workers are:

- Previous offences against children

- If the Governors/Trustees have reservations about an individuals behaviour, lifestyle, attitudes, and spiritual commitment.

- If the Governors/Trustees have any reasons to doubt a worker's suitability for the job.

All new staff will be expected to read the school Code of Conduct Policy and all policies concerning Child Protection and Safeguarding as part of their Induction Process, including the behaviour policy, the safeguarding response to children who go missing from education, and the identity of the DSL and Deputy DSL.

All new staff will need to complete a Basic Awareness Course on Safeguarding and Child Protection, renewable every three years.

The school will keep this information on all staff members as to whether or not the following checks have been carried out or certificates obtained, and the date on which the checks were completed, in a single central record.

Staff are to be informed at interview that the school may review the DBS automatic updates yearly, with prior consent from staff, or ask for a signed declaration regarding any convictions, cautions, reprimands or warnings which have been recorded on a police central record, (includes 'spent' and 'unspent' convictions) or if any information is held locally by police forces

that are grounds to be considered relevant, since their last declaration. This includes any information that may be held on the DBS's children and adults barred list.

If an applicant's criminal record check reveals details of past cautions and/or convictions the following procedures will be followed:

- If the certificate simply confirms what the applicant has already disclosed, and we have already taken this information into account when making the offer of employment, we will confirm the offer of employment.

- If our decision to recruit an applicant depends upon approval from a senior staff member, we shall ensure that the decision maker has all the relevant information to hand in order to make a fair and balanced decision. This may include the applicant's initial disclosure, a disclosure statement, and any other relevant information they may have provided in the interim that may inform a risk assessment.

- If the certificate reveals information that we were not expecting or that the applicant had not previously disclosed, further consideration may be necessary. *See the 'Appointment of Staff and Safer Recruitment Policy'*.

At least one person conducting an interview will have completed safer recruitment training.

Should the school take on Trainee/Student Teachers written confirmation will be obtained from the provider that it has carried out all pre-appointment checks that the school would otherwise be required to perform.

Disqualification

Under section 76(3) schools are prohibited from employing a disqualified person in connection with relevant childcare provision in the settings set out in the relevant offences and orders section of the *Disqualification under the Childcare Act 2006*, unless the individual in question has been granted a waiver by Ofsted for the role they wish to undertake. An employer commits an offence if they contravene section 76(3), except if they prove that they did not know, and had no reasonable grounds for believing, that the person they employed was disqualified.

Disqualification by Association

Disqualification by Association applies if a person is living in the same household where another person who is disqualified lives or is employed (disqualification 'by association') as specified in regulation 9 of the 2018 regulations. Under the 2018 regulations, schools are no longer required to establish whether a member of staff providing, or employed to work in childcare, is disqualified by association.

However, there is now an expectation for all staff to inform the school where their relationships and associations, both within and outside of the workplace (including online), may have implications for the safeguarding of children in the school.

If your circumstances change you must inform the school.

ONLINE & E-SAFETY POLICY

This policy should be read in conjunction with the following guidance:

- Data Protection
- Keeping Children Safe in Education 2021

INTRODUCTION

At Phoenix Academy**,** we understand the responsibility to educate our pupils on online safety issues (e-safety); teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Online safety is a key part of safeguarding so that young people do not see the internet as a separate part of their lives. The school will ensure that online safety is delivered as part of the curriculum on a regular basis.

Internet, mobile and digital technologies in the 21st Century are essential resources to support learning and teaching, as well as playing an important role in the everyday lives of children, young people, and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Internet, mobile and digital technologies cover a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of internet, mobile and digital technologies within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging, and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies, and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much internet, mobile and digital technologies, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these technologies and that some have minimum age requirements (13 years in most cases).

Schools hold personal data on learners, staff, and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, Trustees/Governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

DATA PROTECTION

Phoenix Academy holds a separate Data Protection Policy, including GDPR

MONITORING

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record, and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video, or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards, and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

BREACHES

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software, or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

For pupils, reference will be made to the school's behaviour policy.

INCIDENT REPORTING

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of internet, mobile and digital technologies must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment, or data (including remote access ID and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows: Paul Kelly & Gareth Hawkes

Please refer to the relevant section on Incident Reporting, e-Safety Incident Log & Infringements.

COMPUTER VIRUSES

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

- Never interfere with any anti-virus software installed on school ICT equipment.

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

DATA SECURITY

The accessing and appropriate use of school data is something that the school takes very seriously.

Security of Confidential / Personal Data - Electronic and Paper

It is critical that the school considers the safety of confidential / personal data removed from a school site (electronic and paper).

Possible Statements:

- We will ensure that **ALL** staff are aware of how to handle sensitive or personal information.
- Storage devices such USB sticks are best encrypted in their entirety.
- Staff laptops that hold personal data should have an encrypted 'container' created where all sensitive data should be stored.
- Backup media must always be kept secure.

SECURITY

- The school gives relevant staff access to its Management Information System, with a unique username and password.
- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibility when accessing school data.
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use.
- Staff keep all school related data secure. This includes all personal, sensitive, confidential, or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential, and classified information contained in documents copied, scanned, or printed. This is particularly important when shared copiers (multi-function print, scan, and copiers) are used

PROTECTIVE MARKING OF OFFICIAL INFORMATION

Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them, in line with local business processes.

- There is no requirement to mark routine OFFICIAL information.
- Optional descriptors can be used to distinguish specific type of information.
- Use of descriptors is at an organisation's discretion.
- Existing information does not need to be remarked.

In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL–SENSITIVE'**

RELEVANT RESPONSIBLE PERSONS

Senior members of staff should be familiar with information risks and the school's response. Sometimes called a SIRO, there should be a member of the senior leadership team who has the following responsibilities:

- they lead on the information risk policy and risk assessment
- they advise school staff on appropriate use of school technology
- they act as an advocate for information risk management

The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support relevant responsible staff members in their role.

The SIRO in this school is Gareth Hawkes

INFORMATION ASSET OWNER (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information, and special educational needs data. A responsible member of staff should be able to identify across the school:

- what information is held, and for what purposes;
- what information needs to be protected, how information will be amended or added to over time;
- who has access to the data and why; and
- how information is retained and disposed of.

As a result, this manager can manage and address risks to the information and make sure that information handling complies with legal requirements. In a Secondary School, there may be several individuals, whose roles involve such responsibility.

However, it should be clear to all staff that the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

The IAO in this school is Gareth Hawkes

DISPOSAL OF REDUNDANT ICT EQUIPMENT POLICY

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the

storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen

- Disposal of any ICT equipment will conform to:

  The Waste Electrical and Electronic Equipment Regulations 2006

  The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

  http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

  http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

  http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

  Data Protection Act 2018

  ico education-data

  Electricity at Work Regulations 1989

  http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
- The school's disposal record will include:
  - Date item disposed of
  - Authorisation for disposal, including:
    - verification of software licensing
    - any personal data* likely to be held on the storage media?
  - How it was disposed of e.g., waste, gift, sale
  - Name of person & / or organisation who received the disposed item

* If personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner Website

https://ico.org.uk/

Data Protection Act – data protection guide

https://ico.org.uk/for-organisations/education/

EMAIL

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsible online.

MANAGING E-MAIL

- The school gives all staff & Trustees/Governors their own e-mail account to use for all school business as a work-based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

- Staff & Trustees/Governors should use their school email for all professional communication.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged, if necessary, e-mail histories can be traced. The school email account should be the account that is used for all school business

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses

- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school'. The responsibility for adding this disclaimer lies with the account holder

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper

- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher/Principal or Senior Administrator

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes

- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
    - Delete all e-mails of short-term value
    - Organise e-mail into folders and carry out frequent housekeeping on all folders and archives
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail
- Staff must inform (the e-Safety coordinator or Head Teacher/Principal) if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the Computing Programme of Study
- In whatever way you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

SENDING E-MAILS

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section *E-Mailing Personal, Sensitive, Confidential or Classified Information*
- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal advertising

RECEIVING E-MAILS

- Check your e-mail regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; consult your network manager first
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

- The automatic forwarding and deletion of e-mails is not allowed

E-MAILING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION

Where your conclusion is that e-mail must be used to transmit such data obtain express consent from your Head Teacher/Principal/Senior Administrator to provide the information by e-mail and exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

- Encrypt and password protect.
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document **attached** to an e-mail
- Provide the encryption key or password by a **separate** contact with the recipient(s)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

EQUAL OPPORTUNITIES: PUPILS WITH ADDITIONAL NEEDS

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-Safety rules.

However, staff should be aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration should be given to group interactions when raising awareness of e-Safety. Internet activities should be planned and well managed for these children and young people.

E-SAFETY ROLES AND RESPONSIBILITIES

As e-Safety is an important aspect of strategic leadership within the school, the Head Teacher/Principal and Trustees/Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named e-Safety Safeguarding Officer in this school is Name of Staff who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post.

It is the role of the e-Safety Safeguarding Officer to keep abreast of current issues and guidance through organisations such as the LEA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Trustees/Governors are updated by the e-Safety Safeguarding Officer and all Trustees/Governors understand the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, Trustees/Governors, visitors, and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

E-SAFETY IN THE CURRICULUM

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum, and we continually look for new opportunities to promote e-Safety.

Possible statements

- The school has a framework for teaching internet skills in Computing/ICT/ PSHE lessons (*state which, and where it can be found*.)
- The school provides opportunities within a range of curriculum areas to teach about Online Safety.
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling, and appropriate activities.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e., parent/ carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum *(state examples, i.e., Year 5 QCA unit 5c. Year 8 ICT and PSHE units)*

E-SAFETY SKILLS DEVELOPMENT FOR STAFF

Possible statements

- Our staff receive regular information and training on e-Safety and how they can promote the 'Stay Safe' online messages in the form of *(state how)*
- Details of the ongoing staff training programme can be found *(state where)*
- New staff receive information on the school's acceptable use policy as part of their

induction

- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community (see e-Safety Coordinator)

- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

MANAGING THE SCHOOL E-SAFETY MESSAGES

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used

- The e-Safety policy will be introduced to the pupils at the start of each school year

- E-Safety posters will be prominently displayed

- The key e-Safety advice will be promoted widely through school displays, newsletters, class activities and so on

- We will participate in Safer Internet Day every February.

INCIDENT REPORTING, E-SAFETY & INFRINGEMENTS

INCIDENT REPORTING

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person or e-Safety Coordinator. Additionally, all security breaches, lost/stolen equipment, or data (including remote access ID and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Information Asset Owner.

E-SAFETY INCIDENT LOG

Some incidents may need to be recorded if they relate to a bullying, extremism, or racist incident.

MISUSE AND INFRINGEMENTS

COMPLAINTS

Complaints and/ or issues relating to e-Safety should be made to the e-Safety Safeguarding Officer or Headteacher/Principal.

All incidents should be logged.

INAPPROPRIATE MATERIAL

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety Safeguarding Officer
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
- Users are made aware of sanctions relating to the misuse or misconduct by induction and ongoing training.

INTERNET ACCESS

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas, and publish material which makes it both an invaluable resource for education, business, and social interaction, as well as a potential risk to young and vulnerable people.

MANAGING THE INTERNET

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity

- Staff will preview any recommended sites, online services, software, and apps before use

- Searching for images through open search engines is discouraged when working with pupils

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources

- All users must observe copyright of materials from electronic resources

INTERNET USE

- You must not post personal, sensitive, confidential, or classified information or disseminate such information in any way that may compromise the intended restricted audience

- Do not reveal names of colleagues, pupils, others, or any other confidential information acquired through your job on any social networking site or other online application

- On-line gambling or gaming is not allowed

It is at the Principal's/Head Teacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

INFRASTRUCTURE

- Our school employs some additional web-filtering which is the responsibility of **Gareth Hawkes** who is the school's Network Manager

- IT use is monitored using a pro-active monitoring system. *It is a requirement to have such a system in place*

- However, the school will avoid internet filter 'over-block' as this may place 'unreasonable restrictions on what children can be taught'.

- Phoenix Academy is aware of its responsibility when monitoring staff communication under current legislation and considers; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required

- The school does not allow pupils access to internet logs

- The school uses management control tools for controlling and monitoring workstations

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate

- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up to date on all school machines

- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is neither the school's responsibility nor the network managers to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media, it must be given to Paul Kelly for a safety check first

- Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the Headteacher/Principal/ Network Manager/ICT subject leader

- If there are any issues related to viruses or anti-virus software, the network manager should be informed by phone or in person.

MANAGING OTHER ONLINE TECHNOLOGIES

Online technologies (including social networking sites, if used responsibly both outside and within an educational context) can provide easy to use, creative, collaborative, and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture, and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking and online

games websites to pupils within school

- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online

- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)

- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals

- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online

- Our pupils are asked to report any incidents of Cyberbullying to the school

- Staff may only create blogs, wikis, or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher

- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

PARENTAL INVOLVEMENT

We believe that it is essential for parents/carers to be fully involved with promoting e-Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss e-Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

Possible statements

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-Safety policy by *(state how)*

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school

- Parents/carers are required to decide as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)

- Parents/carers are expected to sign an acceptable use agreement

- The school disseminates information to parents relating to e-Safety where appropriate in the form of: (amend according to what you do)

    - Information evenings
    - Practical training sessions e.g., current e-Safety issues
    - Posters

- School website information
- Newsletter items

PASSWORDS AND PASSWORD SECURITY

PASSWORDS

- **Always use your own** personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else**. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- **Never tell a child or colleague your password**
- **If you aware of a breach of security with your password or account inform Gareth Hawkes immediately**
- Passwords must contain a minimum of six characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers, and symbols
- User ID and passwords for staff and pupils who have left the school are removed from the system within 14 days

If you think your password may have been compromised or someone else has become aware of your password report this to your Head Teacher/Principal/Senior Administrator/Network Manager

PASSWORD SECURITY

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

Possible statements

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security
- Users are provided with an individual network, email, learning platform and

Management Information System log-in username. They are also expected to use a personal password and keep it private

- Pupils are not permitted to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers, or others

- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is 15 minutes

- Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer)

In our school, all ICT password policies are the responsibility of Gareth Hawkes and all staff and pupils are expected to comply with the policies at all times.

ZOMBIE ACCOUNTS

'Zombie accounts' refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left

- Prompt action on disabling accounts will prevent unauthorized access

- Regularly change generic passwords to avoid unauthorised access

PERSONAL OR SENSITIVE INFORMATION

PROTECTING PERSONAL, SENSITIVE, CONFIDENTIAL AND CLASSIFIED INFORMATION

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential, and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential, or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential, and classified information contained in documents you copy, scan, or print. This is particularly important when shared Copiers (multi-function print, scan, and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager

- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential, or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

STORING/TRANSFERRING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION USING REMOVABLE MEDIA

- Ensure removable media is purchased with encryption
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential, or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Guidance on How to Encrypt Files can be found on the ICO website:

https://ico.org.uk/media/for-organisations/encryption-1-0.pdf

REMOTE ACCESS Remove if this is not used within your school

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g., do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Always protect school information and data, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

SAFE USE OF IMAGES

TAKING OF IMAGES AND FILM

The following applies to all parts of the school including the Early Years and Reception class.

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Head Teacher/Principal, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff, and others without advance permission from the Head Teacher/Principal
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication

CONSENT OF ADULTS WHO WORK AT THE SCHOOL

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

PUBLISHING PUPIL'S IMAGES AND WORK

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school website
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- on the school's learning platform or Virtual Learning Environment
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e., exhibition promoting the school
- general media appearances, e.g., local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g., divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the ICT Manager or Head Teacher has authority to upload to the internet.

STORAGE OF IMAGES

- In line with GDPR images are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time.

- Images/ films of children are stored on the school's network

- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head Teacher/Principal

- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource

- Gareth Hawkes & Paul Kelly have the responsibility of deleting the images when they are no longer required.

- Images of past students can remain on the school website if permission is granted by the parent/guardian or if the student has turned over 18.

WEBCAMS AND CCTV

- The school does not use webcams.

VIDEO CONFERENCING

- Permission is sought from parents and carers if their children are involved in video conferences with endpoints outside of the school

- All pupils are supervised by a member of staff when video conferencing

- The school keeps a record of video conferences, including date, time, and participants

- Approval from the Head Teacher/Principal is sought prior to all video conferences within school to end-points beyond the school

- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences

- No part of any video conference is recorded in any medium without the written

consent of those taking part

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS (previously CRB) checked

- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

SCHOOL ICT EQUIPMENT INCLUDING PORTABLE & MOBILE ICT EQUIPMENT AND REMOVABLE MEDIA

SCHOOL ICT EQUIPMENT

- As a user of the school ICT equipment, you are responsible for your activity

- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory

- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available

- Ensure that all ICT equipment that you use is kept physically secure

- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files, or data. This is an offence under the Computer Misuse Act 1990

- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network

- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or another portable device. If it is necessary to do so the local drive must be encrypted

- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles

- Privately owned ICT equipment should not be used on a school network

- On termination of employment, resignation, or transfer, return all school ICT equipment to the school. You must also provide details of all your system logons so that they can be disabled

- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential, or classified information is disclosed to any unauthorised person

- All ICT equipment allocated to staff must be authorised by the Head

Teacher/Principal/Senior Administrator

- maintaining control of the allocation
- recovering and returning equipment when no longer needed

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

PORTABLE & MOBILE ICT EQUIPMENT

This section covers such items as laptops, mobile devices, and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches, or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed, and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

MOBILE TECHNOLOGIES

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

PERSONAL MOBILE DEVICES (INCLUDING PHONES)

- The school allows staff to bring in personal mobile phones and devices for their own

use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device

- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent

- This technology may be used for educational purposes, as mutually agreed with the Head Teacher/Principal. The device user, in this instance, must always ask the prior permission of the bill payer

- The school is not responsible for the loss, damage, or theft of any personal mobile device

- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

- Never use a hand-held mobile phone whilst driving a vehicle

SCHOOL PROVIDED MOBILE DEVICES (INCLUDING PHONES)

- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community

- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used

- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

- Never use a hand-held mobile phone whilst driving a vehicle

TELEPHONE SERVICES

- You may make or receive personal telephone calls provided:

    1. They are infrequent, kept as brief as possible and do not cause annoyance to others

    2. They are not for profit or to premium rate services

    3. They conform to this and other relevant HCC and school policies.

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may

seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases

- Ensure that your incoming telephone calls can be handled at all times

- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask Paul Kelly

REMOVABLE MEDIA

If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section ‘

STORING/TRANSFERRING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION USING REMOVABLE MEDIA

- Always consider if an alternative solution already exists

- Only use recommended removable media

- Encrypt and password protect

- Store all removable media securely

Removable media must be disposed of securely by your ICT support team

SOCIAL MEDIA

Facebook, Twitter, and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school doesn’t currently use Facebook and Twitter to communicate with parents and carers.

- Staff are not permitted to access their personal social media accounts using school equipment at any time during school hours

- Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of social media

- Pupils are not permitted to access their social media accounts whilst at school

- Pupils in Years 10 / 11 are permitted to access their personal social media account using their own device (i.e., mobile phone) outside of lessons

- Staff, Trustees/Governors, pupils, parents, and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others

- Staff, Trustees/Governors, pupils, parents, and carers are aware that the information, comments, images, and video they post online can be viewed by others, copied, and stay online forever

- Staff, Trustees/Governors, pupils, parents, and carers are aware that their online

behaviour should always be compatible with UK law

SERVERS

Phoenix Academy abides by the following criteria:

- Always keep servers in a locked and secure environment
- Limit access rights
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Backup tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Backup tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure

SYSTEMS AND ACCESS

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential, or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential, or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips, or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act, and the Disability Discrimination Act)

- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying, or distributing any material that is protected under the Copyright, Designs and Patents Act 1998

It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

ACCEPTABLE USE POLICIES

See Separate documents

SHARING OF NUDES AND SEMI-NUDES

Also known as 'Sexting' or 'Youth-produced sexual imagery'

This policy is linked to the school's Safeguarding and Child Protection policies.

Further advice may be found in the UKCIS document 'Sharing nudes and semi-nudes'

INTRODUCTION

Consensual and non-consensual sharing of nudes and semi-nudes images and or videos.

The term 'sharing nudes and semi-nudes' is used to mean the sending or posting of nude or semi-nude images, videos, or live streams by young people under the age of 18 online. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's Airdrop which works offline.

The term 'nudes' is used as it is most commonly recognised by young people and more appropriately covers all types of image sharing incidents. Alternative terms used by children and young people may include 'dick pics' or 'pics'.

The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated. Such images may be created and shared consensually by young people who are in relationships, as well as between those who are not in a relationship. It is also possible for a young person in a consensual relationship to be coerced into sharing an image with their partner. Incidents may also occur where:

- children and young people find nudes and semi-nudes online and share them claiming to be from a peer
- children and young people digitally manipulate an image of a young person into an existing nude online
- images created or shared are used to abuse peers e.g., by selling images online or obtaining images to share more widely without consent to publicly shame

Alternative definitions

Many professionals may refer to 'nudes and semi-nudes' as:

- youth produced sexual imagery or 'youth involved' sexual imagery
- indecent imagery. This is the legal term used to define nude or semi-nude images and videos of children and young people under the age of 18.
- 'sexting'. Many adults may use this term, however some young people interpret sexting as 'writing and sharing explicit messages with people they know' rather than sharing images
- image-based sexual abuse. This term may be used when referring to the non-consensual sharing of nudes and semi-nudes

Terms such as 'revenge porn' and 'upskirting' are also used to refer to specific incidents of nudes and semi-nudes being shared. However, these terms are more often used in the context of adult-to-adult non-consensual image sharing offences

Due to the many different types of sexual imaging, it is likely that no two cases will be the same. It is necessary to carefully consider each case on its own merit. However, it is important that Name of School applies a consistent approach when dealing with an incident to help protect young people and the school, and the response should always be guided by the 'principle of proportionality'. The primary concern should always be the welfare and protection of the young people involved. For this reason, the Designated Safeguarding Lead (or Headteacher in the absence of the DSL) needs to be informed of any 'sexual imaging' incidents. The range of contributory factors in each case also needs to be considered in order to determine an appropriate and proportionate response. All colleagues are expected to be aware of this policy.

THE LAW

Indecent images of children

Responding to incidents of sharing nudes and semi-nudes is complex because of its legal status. Making, possessing, and distributing any imagery of someone under 18 which is 'indecent' is illegal. This includes imagery of yourself if you are under 18.

The relevant legislation is contained in the Protection of Children Act 1978 (England and Wales) as amended in the Sexual Offences Act 2003 (England and Wales).

Specifically:

- it is an offence to possess, distribute, show, and make indecent images of children
- the Sexual Offences Act 2003 (England and Wales) defines a child, for the purposes of indecent images, as anyone under the age of 18

'Indecent' is not defined in legislation. When cases are prosecuted, the question of whether any photograph of a child is indecent is for a jury, magistrate or district judge to decide based on what is the recognised standard of propriety

Indecent imagery does not always mean nudity; however, images are likely to be defined as such if they meet one or more of the following criteria:

- nude or semi-nude sexual posing e.g., displaying genitals and/or breasts or overtly sexual images of young people in their underwear
- someone nude or semi-nude touching themselves in a sexual way
- any sexual activity involving a child
- someone hurting someone else sexually
- sexual activity that includes animals

Non-consensual image sharing

- The non-consensual sharing of private sexual images or videos with the intent to cause distress is also illegal. The relevant legislation is contained in section 33 of the Criminal Justice and Courts Act 2015.

HANDLING INCIDENTS

STEP 1 – INITIAL RESPONSE

All schools and colleges are required to have an effective child protection policy in place. It is best practice and recommended for out-of-school settings to also have a child protection policy in place.

The policy should reflect the education setting's approach to incidents of nudes and semi-nudes being shared and staff should respond to such incidents in line with it.

When an incident involving nudes and semi-nudes comes to the attention of any member of staff in an education setting:

- the incident should be referred to the DSL (or equivalent) as soon as possible
- the DSL (or equivalent) should hold an initial review meeting with appropriate staff. This may include the staff member(s) who heard the disclosure and the safeguarding or leadership team who deal with safeguarding concerns
- there should be subsequent interviews with the children or young people involved (if appropriate)
- parents and carers should be informed at an early stage and involved in the process in order to best support the child or young person unless there is good reason to believe that involving them would put the child or young person at risk of harm
- A referral should be made to children's social care and/or the police immediately if there is a concern that a child or young person has been harmed or is at risk of immediate harm at any point in the process

An initial review meeting should be held to consider the initial evidence and aim to establish:

- whether there is an immediate risk to any child or young person
- if a referral should be made to the police and/or children's social care
- if it is necessary to view the image(s) in order to safeguard the child or young person – **in most cases, images or videos should not be viewed**
- what further information is required to decide on the best response
- whether the image(s) has been shared widely and via what services and/or platforms. This may be unknown
- whether immediate action should be taken to delete or remove images or videos from devices or online services
- any relevant facts about the children or young people involved which would influence risk assessment
- if there is a need to contact another education, setting or individual
- whether to contact parents or carers of the children or young people involved - in most cases they should be involved

Assessing the risks once the images have been shared

The circumstances of incidents can vary widely. If at the initial review stage, a decision has been made not to refer to police and/or children's social care, the DSL (or equivalent) should conduct a further review (including an interview with any child or young person involved) to establish the facts and assess the risks, referring back to any relevant assessment tools.

When assessing the risks and determining whether a referral is needed, the following should be also considered:

- why was the nude or semi-nude shared? Was it consensual or was the child or young person put under pressure or coerced?
- has the nude or semi-nude been shared beyond its intended recipient? Was it shared without the consent of the child or young person who produced the image?
- has the nude or semi-nude been shared on social media or anywhere else online? If so, what steps have been taken to contain the spread?
- how old are any of the children or young people involved?
- did the child or young person send the nude or semi-nude to more than one

  person?
- do you have any concerns about the child or young person's vulnerability?
- are there additional concerns if the parents or carers are informed?

These questions will help the DSL (or equivalent) decide whether a child or young person is at risk of harm, in which case a referral will be appropriate, whether additional information or support is needed from other agencies or whether the education setting can manage the incident and support any child or young person directly. DSLs (or equivalent) should always use their professional judgement in conjunction with that of their colleagues to assess incidents.

STEP 2 - SEARCHING A DEVICE – VIEWING THE IMAGERY

Please refer to the school's Search and Confiscation Policy which is based on the most current legislation: The 2011 Education Act.

The policy allows for a device to be examined, confiscated, and securely stored if there is reason to believe it contains indecent images or extreme pornography. When searching a mobile device, the following conditions should apply:

- The action is in accordance with the school's policies regarding Safeguarding and Searching and Confiscation.
- The search is conducted either by the head teacher or a person authorised by them (or Deputy Head or Designated Safeguarding Lead) and one other person
- A member of the safeguarding team should normally be present
- The search should normally be conducted by a member of the same gender as the person being searched. However, if the image being searched for is likely to be of a different gender to the person 'in possession' then the device should only be viewed by a member of the same gender as the person whose image it is.

If any illegal images of a young person are found the Safeguarding Team will discuss this with the Police (see Appendices 1, 2 and 3).

The Association of Chief Police Officers (ACPO) advise that as a general rule it will almost always be proportionate to refer any incident involving 'aggravated' sharing of images to the Police, whereas purely 'experimental' conduct may be proportionately dealt with without such referral, most particularly if it involves the young person sharing images of themselves.

'Experimental conduct' commonly refers to that shared between two individuals (e.g., girlfriend and boyfriend) with no intention to publish the images further (see Supplement 2). Coercion is not a feature of such conduct, neither are requests for images sent from one person to multiple other young persons.

Any conduct involving, or possibly involving, the knowledge or participation of adults should always be referred to the police.

If an 'experimental' incident is not referred to the Police, the reasons for this should be recorded in the school's 'Safeguarding Incidents Log'.

Never search a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the student/young person UNLESS there is clear evidence to suggest not to do so would impede a police inquiry. Always put the young person first. Instead rely on the description by the young person, secure the advice and contact the Police.

Staff and parents or carers must not intentionally view any nudes and semi-nudes unless there is good and clear reason to do so as outlined below. Wherever possible, responses to incidents should be based on what DSLs (or equivalents) have been told about the content of the imagery.

It is important that all members of staff are clear on what they can and can't do in relation to viewing nudes and semi-nudes and that this is communicated to any child, young person or parent and carer requesting that imagery be viewed.

The decision to view any imagery should be based on the professional judgement of the DSL (or equivalent) and should always comply with the child protection policy and procedures of the education setting. Imagery should never be viewed if the act of viewing will cause significant distress or harm to any child or young person involved.

If a decision is made to view imagery, the DSL (or equivalent) would need to be satisfied that viewing:

- is the only way to make a decision about whether to involve other agencies because it is not possible to establish the facts from any child or young person involved
- is necessary to report it to a website, app, or suitable reporting agency (such as the IWF) to have it taken down, or to support the child or young person or parent or carer in making a report
- is unavoidable because a child or young person has presented it directly to a staff member or nudes or semi-nudes have been found on an education setting's device or network

If it is necessary to view the imagery, then the DSL (or equivalent) should:

- never copy, print, share, store or save them; this is illegal. If this has already happened, please contact your local police for advice and to explain the circumstances

- discuss the decision with the headteacher or a member of the senior leadership team
- make sure viewing is undertaken by the DSL (or equivalent) or another member of the safeguarding team with delegated authority from the headteacher or a member of the senior leadership team
- make sure viewing takes place with another member of staff present in the room, ideally the headteacher or a member of the senior leadership team. This staff member does not need to view the images
- wherever possible, make sure viewing takes place on the premises of the education setting, ideally in the headteacher or a member of the senior leadership team's office
- make sure wherever possible that they are viewed by a staff member of the same sex as the child or young person in the images
- record how and why the decision was made to view the imagery in the safeguarding or child protection records, including who was present, why the nudes or semi-nudes were viewed and any subsequent actions. Ensure this is signed and dated and meets any appropriate wider standards e.g., such as those set out in statutory safeguarding guidance and local authority policies and procedures
- if any devices need to be taken and passed onto the police, confiscate the device(s), and call the police. The device should be disconnected from Wi-Fi and data and turned off immediately to avoid imagery being removed from the device remotely through a cloud storage service. The device should be placed in a secure place, for example in a locked cupboard or safe until the police are able to come and collect it

Informing parents and carers

- Parents or carers should be informed and involved in the process at an early stage unless informing them will put a child or young person at risk of harm. Any decision not to inform the parents or carers should be made in conjunction with other services such as children's social care and/or the police, who would take the lead in deciding when they should be informed.
- Where appropriate, DSLs (or equivalents) should support any child or young person involved with determining the best approach for informing parents and carers and allow them to be a part of this process if they want to be.

If there is an indecent image of a child on a website or a social networking site, then the Safeguarding Team will report the image to the site hosting it. Under normal circumstances the team would follow the reporting procedures on the respective website; however, in the case of a sexual imaging incident involving a child or young person where it may be felt that they may be at risk of abuse then the team will report the incident directly to CEOP: www.ceop.police.uk/ceop-report, so that law enforcement can make an assessment, expedite the case with the relevant provider and ensure that appropriate action is taken to safeguard the child.

Once the DSL has enough information, the decision should be made whether to deal with the matter in school or refer it to the police/social care. All information and decision-making should be recorded in line with school policy. If the incident has been dealt with in school, a further review should be held to assess risks.

The DSL should always refer to the police or social care if incident involves:

- an adult
- coercion, blackmail, or grooming
- concerns about capacity to consent, [e.g., SEN]
- images show atypical sexual behaviour for the child's developmental stage
- violent acts are depicted
- image shows sex acts and includes a child under 13
- a young person at risk of immediate harm as a result of the disclosure (for example, self-harm or suicide)

STEP 3 - WHAT TO DO AND NOT DO WITH THE IMAGE

If the image has been shared across a personal mobile device:

Always

- Confiscate and secure the device(s). Close down or switch the device off as soon as possible. This may prevent anyone removing evidence 'remotely'.

Never

- View the image unless there is a clear reason to do so or view it without an additional adult present (this additional person does not need to view the image and certainly should not do so if they are of a different gender to the person whose image has been shared). The viewing of an image should only be done to establish that there has been an incident which requires further action.
- Send, share, or save the image anywhere (**this is illegal)**
- Allow students to do any of the above

If the image has been shared across a school network, a website, or a social network:

Always

- Block the network to all users and isolate the image

Never

- Send or print the image
- Move the material from one place to another
- View the image outside of the protocols in the school's safeguarding and child protection policies and procedures.

Deleting images (from devices and social media)

If the school has decided that other agencies do not need to be involved, then consideration should be given to deleting nudes and semi-nudes from devices and online services to limit any further sharing.

In most cases, children and young people should be asked to delete the imagery and to confirm that they have deleted them. They should be given a deadline for deletion across all devices, online storage, or social media sites. They should be reminded that possession of nudes and semi-nudes is illegal. They should be informed that if they refuse or it is later discovered they did not delete the imagery, they are continuing to commit a criminal offence and the police may become involved.

Any decision to search a child or young person's device and delete imagery should be based on the professional judgement of the DSL (or equivalent) and should always comply with the safeguarding or child protection policy and procedures of the education setting. All of these decisions need to be recorded, including times, dates and reasons for decisions

made and logged in the safeguarding records. Parents and carers should also be informed unless this presents a further risk to any child or the young person.

STEP 4 – RECORDING INCIDENTS

All incidents relating to nudes and semi-nudes being shared need to be recorded. This includes incidents that have been referred to external agencies and those that have not. Incidents that have not been reported out to police or children's social care, education settings should record their reason for doing so and ensure it is signed off by the headteacher or setting's manager/leadership team. Please note copies of imagery should not be taken.

Records should be kept in line with statutory requirements set out in Keeping Children Safe in Education, where applicable, and your local safeguarding procedures.

STEP 5 - DECIDING ON A RESPONSE

There may be many reasons why a student has engaged in sexual imaging – it may be a romantic/sexual exploration scenario, or it may be due to coercion.

It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident (see Supplement 1 for definitions). However, as a school it is important that incidents are consistently recorded. It may also be necessary to assist the young person in removing the image from a website or elsewhere.

If indecent images of a young person are found:

- Act in accordance with the Safeguarding policy i.e., inform the Safeguarding Team
- Store the device securely
- The Safeguarding Team should carry out a risk assessment in relation to the young person (Use Appendices 2 and 3 for support)
- The Safeguarding Team will make a referral if needed
- The Safeguarding Team will contact the police (if appropriate). Referrals may be made to Social Care but where a crime may have thought to have taken place the police are the first port of call. Young persons who have engaged in 'experimental sexual imaging' which is contained between two persons will be referred to Social Care for support and guidance. Those who are felt to be victims of 'sexual imaging' will also be referred to Social Care at a point where the police feel that this will not impede an investigation.
- The young person's Supervisor will put the necessary safeguards in place for the student, e.g., they may need counselling support or immediate protection.
- Inform parents and/or carers about the incident and how it is being managed.

Reporting nudes and semi-nudes online

Children and young people may need help and support with the removal of nudes and semi-nudes from devices and social media, especially if they are distressed. Most online service providers offer a reporting function for account holders, and some offer a public reporting function to enable a third party to make a report on behalf of the child or young person. More information can be found on individual providers' websites where they should make public their Terms of Service and process for reporting.

In the event that a site has no reporting function and if the content is a sexual image of someone under 18, you can report it to the Internet Watch Foundation (IWF). You can report directly to the IWF here: www.iwf.org.uk.

Children and young people can use the IWF and Childline's Report Remove tool to report images and videos they are worried have been, or might be, shared publicly at www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile- safety/sexting/report-nude-image-online/. The tool helps children and young people to report an image shared online, to see if it is possible to get the image removed. This must be done as soon as possible in order to minimise the number of people that have seen the picture.

If you are concerned that a child or young person is being sexually abused, exploited, or groomed online you should report to NCA-CEOP: www.ceop.police.uk/safety-centre.

Supporting parents and carers

For advice on supporting parents and carers see the UKCIS document 'Sharing nudes and semi-nudes'

STEP 6 - CONTAINMENT AND PREVENTION

The young persons involved in 'sexual imaging' may be left feeling sensitive and vulnerable for some time. They will require monitoring by and support from their Guidance/Pastoral teams.

Where cases of 'sexual imaging' become widespread or there is thought to be the possibility of contagion then the school will reinforce the need for safer 'online' behaviour using a variety of resources.

Other staff may need to be informed of incidents and should be prepared to act if the issue is continued or referred to by other students. The school, its students and parents should be on high alert, challenging behaviour and ensuring that the victim is well cared for and protected.

The students' parents should usually be told what has happened so that they can keep a watchful eye over the young person especially when they are online at home.

STEP 7 - REVIEW OUTCOMES AND PROCEDURES WITH THE AIM OF PREVENTING FUTURE INCIDENTS

The frequency or severity of such incidents may be such that the school will need to review its approach. Where this is the case Name of School will do the following:

- ensure that key policies e.g., Safeguarding, Anti- Bullying, Authorised User Policies are still relevant and can meet emerging issues.
- ensure that the school's infrastructure and technologies are robust enough to meet new challenges.
- ensure that both adults and young persons are alerted to the issues such as safety mechanisms, support mechanisms and the legal implications of such behaviour.
- use the Ofsted framework for Behaviour and Safety as a benchmark to test the strength of the school's approach.

Sexual imaging incidents relate to self-generated images on personally owned devices, generally outside of school. Name of School will adopt preventative education strategies for its young people and put in place appropriate staff training to identify and manage incidents. The following are resources currently available:

- CEOP resources at www.thinkuknow.co.uk. There is a film called Exposed and accompanying lesson plans for 11-16 year olds.

- The children's charity Childnet www.childnet-int.org have developed a drama for secondary school-aged children on the issue of sexual imaging.
- The Southwest Grid for Learning have developed a resource for young people: 'So you got naked online' which supports them in knowing what to do if things have gone wrong online. This may be found at: https://swgfl.org.uk/products-services/online-safety/resources/so-you-got-naked-online/

SHARING OF NUDES AND SEMI-NUDES - SUPPLEMENT 1

THE LEGAL POSITION

It is important to be aware that young people involved in sharing sexual videos and pictures may be committing a criminal offence. Specifically, crimes involving indecent photographs (including pseudo images) of a person under 18 years of age fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988. Under this legislation it is a crime to:

- take an indecent photograph or allow an indecent photograph to be taken;
- make an indecent photograph (this includes downloading or opening an image that has been sent via email);
- distribute or show such an image;
- possess with the intention of distributing images;
- advertise; and
- possess such images

While any decision to charge individuals for such offences is a matter for the Crown Prosecution

Service, it is unlikely to be considered in the public interest to prosecute children. However, children need to be aware that they may be breaking the law. Although unlikely to be prosecuted, children and young people who send or possess images may be visited by police and on some occasions, media equipment could be removed. This is more likely if they have distributed images.

The decision to criminalise children and young people for sending these kinds of images is a little unclear and may depend on local strategies. However, the current Association of Chief Police Officers (ACPO) position is that: *'ACPO does not support the prosecution or criminalisation of children for taking indecent images of themselves and sharing them. Being prosecuted through the criminal justice system is likely to be upsetting and distressing for children especially if they are convicted and punished. The label of sex offender that would be applied to a child or young person convicted of such offences is regrettable, unjust and clearly detrimental to their future health and wellbeing.'*

However, there are cases in which children and young people have been convicted and sent to prison. The important thing to remember is that whilst, as a school, we will want to consider the implications of reporting an incident over to the police, it is not our responsibility to make decisions about the seriousness of the matter; that responsibility lies with the Police and the CPS hence the requirement for the school to refer.

In summary sexual imaging is classed as illegal as it constitutes sharing and/or possessing an indecent image of a child.

SHARING OF NUDES AND SEMI-NUDES - SUPPLEMENT 2

DIFFERENT LEVELS OF SEXUAL IMAGING

The following is adapted from Wolak and Finkelhor *'Sexual imaging: A Typology'.* March 2011

Aggravated incidents involving criminal or abusive elements beyond the creation, sending or possession of youth-produced sexual images

- **Adult offenders** develop relationships with and seduce underage teenagers, in criminal sex offences even without the added element of youth-produced images. Victims may be family friends, relatives, community members or contacted via the Internet. The youth produced sexual images generally, but not always, are solicited by the adult offenders.

- **Youth Only**: **Intent to Harm** cases that:
    - arise from interpersonal conflict such as break-ups and fights among friends
    - involve criminal or abusive conduct such as blackmail, threats, or deception
    - involve criminal sexual abuse or exploitation by juvenile offenders.

- **Youth Only: Reckless Misuse** no intent to harm but images are taken or sent without the knowing or willing participation of the young person who is pictured. In these cases, pictures are taken or sent thoughtlessly or recklessly, and a victim may have been harmed as a result, but the culpability appears somewhat less than in the malicious episodes.

Experimental incidents involve the creation and sending of youth-produced sexual images, with no adult involvement, no apparent intent to harm or reckless misuse.

- **Romantic episodes** in which young people in ongoing relationships make images for themselves or each other, and images were not intended to be distributed beyond the pair.

- **Sexual Attention Seeking** in which images are made and sent between or among young people who were not known to be romantic partners, or where one youngster takes pictures and sends them to many others or posts them online, presumably to draw sexual attention.

- **Other:** cases that do not appear to have aggravating elements, like adult involvement, malicious motives, or reckless misuse, but also do not fit into the Romantic or Attention Seeking sub-types. These involve either young people who take pictures of themselves for themselves (no evidence of any sending or sharing or intent to do so) or pre-adolescent children (age 9 or younger) who did not appear to have sexual motives.

SHARING NUDES AND SEMI-NUDES: HOW TO RESPOND TO AN INCIDENT – SUPPLEMENT 3

An overview for all staff working in education settings in England

This document provides a brief overview for frontline staff of how to respond to incidents where nudes and semi-nudes have been shared.

All such incidents should be immediately reported to the Designated Safeguarding Lead (DSL) or equivalent and managed in line with your setting's child protection policies.

The appropriate safeguarding lead person should be familiar with the full 2020 guidance from the UK Council for Internet Safety (UKCIS), ***Sharing nudes and semi-nudes: advice for education settings working with children and young people*** and should **not** refer to this document instead of the full guidance.

What do we mean by sharing nudes and semi-nudes?

In the latest advice for schools and colleges (UKCIS, 2020), this is defined as the sending or posting of nude or semi-nude images, videos, or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's Airdrop which works offline. Alternative terms used by children and young people may include 'dick pics' or 'pics'.

The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated.

This advice does not apply to adults sharing nudes or semi-nudes of under 18-year olds. This is a form of child sexual abuse and must be referred to the police as a matter of urgency.

What to do if an incident comes to your attention

Report it to your Designated Safeguarding Lead (DSL) or equivalent immediately. **Your setting's child protection policy should outline codes of practice to be followed.**

- **Never** view, copy, print, share, store or save the imagery yourself**,** or ask a child to share or download – **this is illegal**.[1]
- If you have already viewed the imagery by accident (e.g., if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
- **Do not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

[1] In exceptional circumstances, it may be necessary for the DSL (or equivalent) only to view the image in order to safeguard the child or young person. That decision should be based on the professional judgement of the DSL (or equivalent).

SAFETY MATTERS

An annual safety review will be held to consider all aspects of safety for children and young people. The school's arrangements to fulfil other safeguarding and welfare responsibilities are as follows:

- Ensure high standards of provision and care for children and learners
- Actively promote equality and diversity
- Tackle bullying and discrimination immediately
- Actively promote British values
- Prevent radicalisation and extremism
- Ensure that all persons know how to complain and understand the process for doing so
- Ensure that children and learners are protected and feel safe.
- Challenge any discriminatory behaviour and give help and support to children about how to treat others with respect
- Consistently promote positive behaviour
- Ensure that all children and learners can identify a trusted adult with whom they can communicate about any concerns, and know that these adults will listen to them and take their concerns seriously
- Ensure that written records are made in a timely way and held securely where adults working with children or learners are concerned about their safety or welfare. Those records will be shared appropriately and, where necessary, with consent.
- Make clear risk assessments
- Oversee the safe use of technology by ensuring that our policies and procedures are adhered to
- Use an Acceptable Use Agreement
- Carefully select and vet staff and volunteers working with children and learners according to statutory requirements.
- Check all staff using Enhanced DBS checks
- Ensure that all staff have regular Child Protection and Safeguarding Training
- Ensure that the Designated Safeguarding Leads undertake training at two-yearly intervals, and in addition receive an update at least yearly
- Ensure that the Deputy DSL is trained to the same standards as the DSL.
- Ensure training allows the DSL to "recognise the additional risks that children with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation and are confident they have the capability to support SEND children to stay safe online".
- Ensure that the Designated Safeguarding Lead and Deputy DSL have job descriptions, where their roles are explicit, with clear cover arrangements. DSLs will be drawn from the senior leadership

team and will be the persons carrying out the day-to-day work of safeguarding and child protection. Their responsibilities will not be delegated to others. See *Appendix 1.*

- Keep the Single Central Record up to date
- Regularly review safeguarding policies and procedures to keep all children and learners safe
- Ensure the school holds more than one emergency contact number for each pupil.

Policy Adopted by Governors/Trustees on: 27th October 2021

By Chair of Governors: 

HELP AND SUPPORT

Our organisation has a legal obligation to protect sensitive information under the Data Protection Act 2018. For more information visit the website of the Information Commissioner's Office https://ico.org.uk/

Advice on e-Safety* - http://www.thegrid.org.uk/eservices/safety/index.shtml

Further guidance* - http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

The Information Management Toolkit for Schools is available at:
https://irms.org.uk/general/custom.asp?page=SchoolsToolkit

Safeguarding Children online – free expert advice: http://www.getsafeonline.org

Review Online (E-Safety) policy and practice at https://360safe.org.uk/

Data Protection Team – email insert your local contact

Resources to support schools with online safety:

- /UKCIS Education for a Connected World.pdf/
- Guidance from the PSHE Association
- Internet Legends by Parent Zone & Google

Numerous organisations are listed in Annex D of KCSIE, that can provide support concerning online safety.

CURRENT LEGISLATION

ACTS RELATING TO MONITORING OF STAFF EMAIL

Data Protection Act 2018

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individual's rights of access to their personal data, compensation, and prevention of processing. The **Data Protection Act 2018** implements the European Union's General Data Protection Regulation (GDPR) in national law,

http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

https://www.legislation.gov.uk/ukpga/2000/23

Human Rights Act 1998

https://www.legislation.gov.uk/ukpga/1998/42

OTHER ACTS RELATING TO ESAFETY

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing, or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality, or ethnic background.

http://www.legislation.gov.uk/ukpga/2006/1

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images

such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of *Working Together to Safeguard Children, 2018* document as part of their child protection packs.

https://www.legislation.gov.uk/ukpga/2003/42

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene, or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent, there is no need to prove any intent or purpose.

http://www.legislation.gov.uk/ukpga/2003/21/section/127

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

https://www.legislation.gov.uk/ukpga/1990/18

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

https://www.legislation.gov.uk/ukpga/1988/27

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film, and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually, a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is

also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

https://www.legislation.gov.uk/ukpga/1988/48

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

https://www.legislation.gov.uk/ukpga/1986/64

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

https://www.legislation.gov.uk/ukpga/1978/37

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

https://www.legislation.gov.uk/ukpga/Eliz2/7-8/66 and
http://www.legislation.gov.uk/ukpga/1964/74

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

https://www.legislation.gov.uk/ukpga/1997/40

ACTS RELATING TO THE PROTECTION OF PERSONAL DATA

Data Protection Act 2018

http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The Freedom of Information Act 2000

https://www.legislation.gov.uk/ukpga/2000/36

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

COUNTER-TERRORISM AND SECURITY ACT 2015 (PREVENT), ANTI-RADICALISATION & COUNTER-EXTREMISM GUIDANCE

https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services

The school holds the document '*The Prevent duty Departmental Advice for Schools and Childcare Providers, June 2015*' on file.

Appendix 1

ROLE AND RESPONSIBILITIES OF THE SCHOOL DESIGNATED SAFEGUARDING LEAD

The School Designated Safeguarding Lead (DSL) is the first point of contact for any member of the school staff who has a concern about the safety and well-being of a student. The DSL and Deputy DSL are most likely to have a complete safeguarding picture and will be the most appropriate individuals to advise on any safeguarding concerns.

The DSL does not need to be a member of the teaching staff but should be a recognised member of the Senior Management Team with the required status and authority to carry out the requirements of the role. Their appointment will be decided by the governing board or proprietor.

Depending on the size and requirements of the school a Deputy Designated Safeguarding Lead should be available. The Deputy is the first point of contact in the absence of the DSL to avoid any unnecessary delays in responding to a student's needs.

The DSL and Deputy DSL are required to undertake child protection training every two years and should supplement this training by attending workshops where available, at least annually. This training should also help the DSL and Deputy DSL recognise the additional risks that children with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation and are confident they have the capability to support SEND children to stay safe online.

Requirements:

- To have the skills and ability to identify signs of abuse.
- To know how to refer concerns to the appropriate investigating agencies.
- Maintain detailed and accurate written records of child protection concerns and ensure they are kept securely.
- Offer support, advice and give a level of expertise to all members of the school staff team.
- Ensure that all staff have access to and understand the school Safeguarding and Child Protection Policy and Procedures.
- To be able to provide basic awareness/child protection training as part of the induction for all new staff in the school and be part of any other relevant training.
- Be responsible with the Principal/Head Teacher for the annual review and update of the School Safeguarding Policy and the presentation of this to the Governing Body.
- Ensure that a copy of the School Safeguarding and Child Protection Policy is available for any parents who request to see it.

- Ensure that the Principal/Head Teacher and Chair of Governors/Trustees are updated on a regular basis about all issues and child protection investigations.

- Ensure that relevant safeguarding files are copied and forwarded appropriately when a child/young person transfers to another school.

- Be part of the team who review and monitor any causes of concern relating to students which are raised in school.

Role and Responsibilities:

Taken from Annex C KCSIE 2021

Manage referrals

The Designated Safeguarding Lead is expected to refer cases:

- of suspected abuse and neglect to the local authority children's social care as required and support staff who make referrals to local authority children's social care;

- to the Channel programme where there is a radicalisation concern as required and support staff who make referrals to the Channel programme;

- where a person is dismissed or left due to risk/harm to a child to the Disclosure and Barring Service as required; and

- where a crime may have been committed to the Police as required. NPCC - When to call the police should help understand when to consider calling the police and what to expect when working with the police.

Work with others

The Designated Safeguarding Lead is expected to:

- act as a source of support, advice, and expertise for all staff;

- act as a point of contact with the three safeguarding partners;

- liaise with the headteacher or principal to inform him or her of issues- especially ongoing enquiries under section 47 of the Children Act 1989 and police investigations;

- as required, liaise with the "case manager" (as per Part four) and the local authority designated officer(s) (LADO) for child protection concerns in cases which concern a staff member;

- liaise with staff (especially teachers, pastoral support staff, school nurses, IT Technicians, senior mental health leads and special educational needs coordinators (SENCOs), or the named person with oversight for SEN in a college and Senior Mental Health Leads) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies so that children's needs are considered holistically;

- liaise with the senior mental health lead and, where available, the Mental Health Support Team, where safeguarding concerns are linked to mental health;

- promote supportive engagement with parents and/or carers in safeguarding and promoting the welfare of children, including where families may be facing challenging circumstances;

- work with the headteacher and relevant strategic leads, taking lead responsibility for promoting educational outcomes by knowing the welfare, safeguarding and child protection issues that children in need are experiencing, or have experienced, and identifying the impact that these issues might be having on children's attendance, engagement and achievement at school or college. This includes:

    - ensure that the school or college knows who its cohort of children who have or have had a social worker are, understanding their academic progress and attainment, and maintaining a culture of high aspirations for this cohort; and,

    - support teaching staff to provide additional academic support or reasonable adjustments to help children who have or have had a social worker reach their potential, recognising that even when statutory social care intervention has ended, there is still a lasting impact on children's educational outcomes.

Information sharing and managing the child protection file

The designated safeguarding lead is responsible for ensuring that child protection files are kept up to date.

Information should be kept confidential and stored securely. It is good practice to keep concerns and referrals in a separate child protection file for each child.

Records should include:

- a clear and comprehensive summary of the concern;

- details of how the concern was followed up and resolved;

- a note of any action taken, decisions reached and the outcome.

They should ensure the file is only accessed by those who need to see it and where the file or content within it is shared, this happens in line with information sharing advice as set out in Part one and Part two of this guidance.

Where children leave the school or college (including in year transfers) the designated safeguarding lead should ensure their child protection file is transferred to the new school or college as soon as possible, and within 5 days for an in-year transfer or within the first 5 days of the start of a new term. This should be transferred separately from the main pupil file, ensuring secure transit, and confirmation of receipt should be obtained. Receiving schools and colleges should ensure key staff such as designated safeguarding leads and SENCOs or the named person with oversight for SEN in colleges, are aware as required.

Lack of information about their circumstances can impact on the child's safety, welfare, and educational outcomes. In addition to the child protection file, the designated safeguarding lead should also consider if it would be appropriate to share any additional information with the new school or college in advance of a child leaving to help them put in place the right support to safeguard this child and to help the child thrive in the school or college. For example, information that would allow the new school or college to continue supporting children who have had a social worker and been victims of abuse and have that support in place for when the child arrives.

Training, knowledge, and skills

The Designated Safeguarding Lead (and any deputies) should undergo training to provide them with the knowledge and skills required to carry out the role. This training should be updated at least every two years. The Designated Safeguarding Lead should undertake Prevent awareness training. Training should provide designated safeguarding leads with a good understanding of their own role, how to identify, understand and respond to specific needs that can increase the vulnerability of children, as well as specific harms that can put children at risk, and the processes, procedures, and responsibilities of other agencies, particularly children's social care, so they:

- understand the assessment process for providing early help and statutory intervention, including local criteria for action and local authority children's social care referral arrangements.
- have a working knowledge of how local authorities conduct a child protection case conference and a child protection review conference and be able to attend and contribute to these effectively when required to do so;
- understand the importance of the role the designated safeguarding lead has in providing information and support to children social care in order to safeguard and promote the welfare of children;
- understand the lasting impact that adversity and trauma can have, including on children's behaviour, mental health, and wellbeing, and what is needed in responding to this in promoting educational outcomes;
- are alert to the specific needs of children in need, those with special educational needs and disabilities (SEND), those with relevant health conditions and young carers;
- understand the importance of information sharing, both within the school and college, and with the three safeguarding partners, other agencies, organisations, and practitioners;
- understand and support the school or college with regards to the requirements of the Prevent duty and are able to provide advice and support to staff on protecting children from the risk of radicalisation;
- are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college;
- can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation and are confident they have the capability to support SEND children to stay safe online;
- obtain access to resources and attend any relevant or refresher training courses; and
- encourage a culture of listening to children and taking account of their wishes and feelings, among all staff, in any measures the school or college may put in place to protect them.

In addition to the formal training set out above, their knowledge and skills should be refreshed (this might be via e-bulletins, meeting other designated safeguarding leads, or simply taking time to read and digest safeguarding developments) at regular intervals, as

required, and at least annually, to allow them to understand and keep up with any developments relevant to their role.

Raise Awareness

The Designated Safeguarding Lead should:

- ensure each member of staff has access to, and understands, the school's or college's child protection policy and procedures, especially new and part-time staff;
- ensure the school's or college's child protection policy is reviewed annually (as a minimum) and the procedures and implementation are updated and reviewed regularly, and work with governing bodies or proprietors regarding this;
- ensure the child protection policy is available publicly and parents are aware of the fact that referrals about suspected abuse or neglect may be made and the role of the school or college in this;
- link with the safeguarding partner arrangements to make sure staff are aware of any training opportunities and the latest local policies on local safeguarding arrangements; and
- help promote educational outcomes by sharing the information about the welfare, safeguarding and child protection issues that children who have or have had a social worker, are experiencing with teachers and school and college leadership staff.

Providing support to staff

Training should support the designated safeguarding lead in developing expertise, so they can support and advise staff and help them feel confident on welfare, safeguarding and child protection matters. This includes specifically to:

- ensure that staff are supported during the referrals processes; and
- support staff to consider how safeguarding, welfare and educational outcomes are
- linked, including to inform the provision of academic and pastoral support.

Understanding the views of children

It is important that children feel heard and understood. Therefore, designated safeguarding leads should be supported in developing knowledge and skills to:

- encourage a culture of listening to children and taking account of their wishes and feelings, among all staff, and in any measures the school or college may put in place to protect them; and
- understand the difficulties that children may have in approaching staff about their circumstances and consider how to build trusted relationships which facilitate communication.

Holding and sharing information

The critical importance of recording, holding, using, and sharing information effectively is set out in Parts one, two and five of this document; and therefore, the designated safeguarding lead should be equipped to:

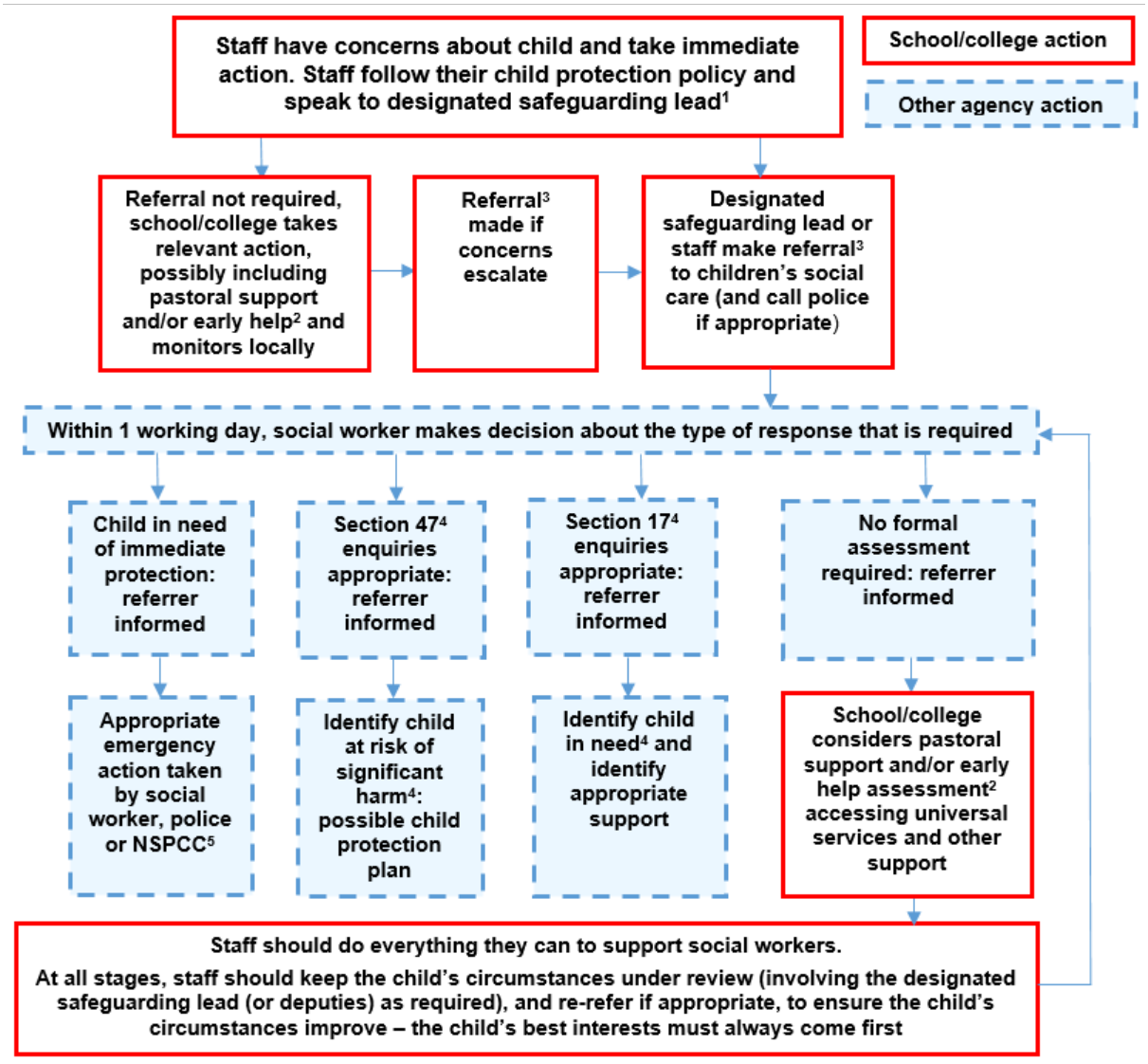
- understand the importance of information sharing, both within the school and college, and with other schools and colleges on transfer including in-year and between

primary and secondary education, and with the safeguarding partners, other agencies, organisations, and practitioners;

- understand relevant data protection legislation and regulations, especially the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR); and,
- be able to keep detailed, accurate, secure written records of concerns and referrals and understand the purpose of this record-keeping.

ACTIONS WHERE THERE ARE CONCERNS ABOUT A CHILD

Please check your own Safeguarding Children Partnership for local advice and change if necessary



[1]In cases which also involve a concern or an allegation of abuse against a staff member, see Part Four of this guidance.
[2]Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of Working Together to Safeguard Children provides detailed guidance on the early help process.
[3]Referrals should follow the process set out in the local threshold document and local protocol for assessment. Chapter one of Working Together to Safeguard Children.
[4]Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Chapter one of Working Together to Safeguard Children.
[5]This could include applying for an Emergency Protection Order (EPO).

Appendix 3

COVID-19 and SAFEGUARDING

Schools must have regard to the statutory safeguarding guidance, **keeping children safe in education** and should refer to the now updated and update safeguarding procedures in line with DfE updates.

https://www.gov.uk/government/publications/actions-for-schools-during-the-coronavirus-outbreak

Online safety

Coronavirus (COVID-19): keeping children safe online - All schools and colleges should continue to consider the safety of their children when they are asked to work online. The starting point for online teaching should be that the same principles as set out in the school's or college's staff behaviour policy (sometimes known as a code of conduct) should be followed. This policy should amongst other things include acceptable use of technologies, staff pupil/student relationships and communication including the use of social media. The policy should apply equally to any existing or new online and distance learning arrangements which are introduced.

Schools and colleges should, as much as is reasonably possible, consider if their existing policies adequately reflect that some children (and in some cases staff) continue to work remotely online. As with the child protection policy, in some cases an annex/addendum summarising key coronavirus related changes may be more effective than re-writing/re-issuing the whole policy.

The principles set out in the **guidance for safer working practice for those working with children and young people in education settings** published by the Safer Recruitment Consortium may help schools and colleges satisfy themselves that their staff behaviour policies are robust and effective. In some areas schools and colleges may be able to seek support from their local authority when planning online lessons/activities and considering online safety.

Schools and colleges should continue to ensure any use of online learning tools and systems is in line with privacy and data protection requirements.

An essential part of the online planning process will be ensuring children who are being asked to work online have very clear reporting routes in place so they can raise any concerns whilst online. As well as reporting routes back to the school or college this should also signpost children to age appropriate practical support from the likes of:

- **Childline** - for support
- **UK Safer Internet Centre** - to report and remove harmful online content
- **CEOP** - for advice on making a report about online abuse

Schools and colleges are likely to be in regular contact with parents and carers. Those communications should continue to be used to reinforce the importance of children being safe online. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online.

Parents and carers may choose to supplement the school or college online offer with support from online companies and in some cases individual tutors. In their communications with parents and carers, schools and colleges should emphasise the importance of securing online support from a reputable organisation/individual who can provide evidence that they are safe and can be trusted to

have access to children.Support for parents and carers to keep their children safe online includes:

- **Thinkuknow** provides advice from the National Crime Agency (NCA) on staying safe online.
- **Parent info** is a collaboration between Parentzone and the NCA providing support and guidance for parents from leading experts and organisations.
- **Childnet** offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support.
- **Internet Matters** provides age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world.
- **London Grid for Learning** has support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online.
- **Net-aware** has support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games.
- **Let's Talk About It** has advice for parents and carers to keep children safe from online radicalisation.
- **UK Safer Internet Centre** has tips, advice, guides and other resources to help keep children safe online, including parental controls offered by home internet providers and safety tools on social networks and other online services.

Government has also provided:

- **Support to stay safe online** includes security and privacy settings, blocking unsuitable content, and parental controls.

The department encourages schools and colleges to share this support with parents and carers.