Safety Policy

Online Safety

POLICY STATEMENT

- Safeguard all individuals within our services settings (Team Members and the People we support) online.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Phoenix community in its use of technology, including mobile and smart technology.
- Uphold the rights of all the People we support to access appropriate online information, which is appropriate to their age and understanding, whilst being protected from harm, abuse and exploitation.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- UNCRC Article 17 – Children have the right to access information from the media.
- UNCRC Article 36 - Children have the right to be kept safe from exploitation.

Document Control			
Policy Code:	GRP 555	Policy Owner:	Quality Team
Version:	25.08_v1.05	Policy Author(s):	Abbie Heard (Quality Manager) Wanda Green (Head of Safeguarding & Quality) Olivia James (Project Manager)
Date ratified:	September 2025		
Review Frequency:	Yearly		
Next review date:	September 2026	Ratifying Committee:	PRG

Document History (last 3 versions)			
Date of Issue	Version No.	Person(s) responsible for change	Nature of Change
August 2025	1.05	Abbie Heard	Legislation updates and review
May 2025	1.04	Abbie Heard	Extensive Review
August 2024	1.03	Abbie Heard	KCSIE updates

CONTENTS

1. Scope

1.1 The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

1.1.1 Content – being exposed to illegal, inappropriate, or harmful content, such as pornography, misinformation, disinformation (incl. fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism.

1.1.2 Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

1.1.3 Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending, and receiving explicit images (e.g., consensual, and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

1.1.4 Commercial exploitation – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

1.2 Legislation and guidance

1.2.1 Phoenix acknowledges the educational, social and entertainment benefits that the internet, mobile phones, computers, laptops, tablets, games consoles and other technologies offer.

1.2.2 We recognise our duty under the Education Act 2002 to make arrangements to ensure that functions are carried out with a view to safeguarding and promoting the welfare of children and comply with The Education (Independent School Standards) Regulations 2014.

1.2.3 Phoenix complies with The Children's Homes (England) Regulations 2015, The Regulation and Inspection of Social Care and Wellbeing Act (Wales) 2016, and the Guide to the Children's Homes Regulations including the quality standards (2015). Phoenix acknowledges the obligations associated with the Children Act 1989, the Human Rights Act 1998 and the Equality Act 2010. We also follow current DfE guidance 'Keeping children safe in education' (England), 'Working together to safeguard children', Keeping Leaners Safe (Wales), HM Government advice 'What to do if you're worried a child is being abused' (2015) and the Local Safeguarding Children Partnership's policies, procedures, guidance, and protocols.

1.2.4 This policy has also been informed by the following guidance:

- CEOP Education, part of the National Crime Agency which aims to reduce the vulnerability of children and young people to online sexual abuse.

  Hwb Online Safety. Welsh Government and Education Wales

  Keeping Children Safe in Education 2025

- Keeping Learners Safe 2022 and its advice for schools on: Teaching online safety in schools

- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- It also refers to the DfE's guidance on protecting children from radicalisation.
- It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, Online Safety Act 2023 and the Equality Act 2010.

1.3 Links with other policies and practices

- PCC019 Safeguarding Policy (Childcare)
- 22 Safeguarding and Child Protection (Education)
- 11 Searches, Screening and Confiscation (Education)
- 25 Police Involvement (Education)
- OCC 4 Safeguarding (College)
- Adult Services 4 Safeguarding People we support
- PCC002 Therapeutic Approach (Behaviour) Policy
- GRP 537 Disciplinary Policy
- GRP 527 Team Member Code of Conduct
- GRP 528 Data protection policy and privacy notices
- GRP 550 Anti Radicalisation Policy
- GRP 555 Acceptable Use of Technology and Social Media Policy.
- GRP 575 Child on Child (Peer-on-Peer)

2. Roles and Responsibilities

2.1.1 All Team Members have important roles and responsibilities to play with regards to online safety.

2.2 The Leadership and Management Teams will:

2.2.1 Ensure that they have read and understand this policy.

2.2.2 Agree and adhere to the terms of the Acceptable Use Policy.

2.2.3 Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.

2.2.4 Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of Conduct, which includes acceptable use of technology.

2.2.5 Ensure that suitable and appropriate filtering and monitoring systems are in place.

2.2.6 Work with the IT Team to monitor the safety/security of organisation systems/networks.

2.2.7 Ensure that online safety is embedded within a progressive curriculum in our educational establishments and our residential settings, which enables all the People we support to develop an age-appropriate understanding of online safety.

2.2.8 Support the Designated Safeguarding Leads/Designated Safeguarding Persons by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.

2.2.9 Ensure that there are robust reporting channels to access regarding online safety concerns, including internal, and external support.

2.2.10 Ensure that appropriate risk assessments are undertaken regarding the safe use of technology whilst auditing and evaluating online safety practice to identify strengths and areas for improvement.

2.2.11 Ensure all equipment and data is correctly archived when not in use and/or when a Team Member/Person we support leaves the organisation.

2.3 The Designated Safeguarding Leads/ Designated Safeguarding Persons will:

2.3.1 Details of the roles of our Designated Safeguarding Leads (DSL/DSP) [and Deputy/Deputies] are set out in our child/adult protection and safeguarding policies as well as relevant job descriptions.

2.3.2 Act as a named point of contact on all online safeguarding issues and liaise with other Team Members or other agencies, as appropriate.

2.3.3 Keep up to date with current research, legislation and trends regarding online safety and communicate this to the various services provided by the Organisation, as appropriate.

2.3.4 Ensure all Team Members receive regular, up-to-date, and appropriate online safety training.

2.3.5 Work with Team Members to coordinate participation in local and national events to promote positive online behaviour, such as *Safer Internet Day*.

2.3.6 Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the therapeutic approaches policy and behaviour support plans.

2.3.7 Maintain records of online safety concerns, as well as actions taken, as part of the individual settings safeguarding recording mechanisms.

2.3.8 Monitor online safety incidents to identify gaps and trends and use this data to update the organisation response (e.g., policies and procedures).

2.3.9 Liaise with other agencies and/or external services if necessary.

2.3.10 Report online safety concerns, as appropriate, to the management teams, and Governing body.

2.4 Child Exploitation and Online Protection (CEOP) Ambassador will:

2.4.1 Attend external training from the CEOP education team.

2.4.2 Deliver training sessions to managers and Team Members within the organisation.

2.4.3 Attend training and/or events to develop their knowledge and skills.

2.4.4 Be a source of up-to-date information on online child sexual abuse within Phoenix.

2.4.5 Use and promote the use of up to date and current National Crime Agency CEOP Education resources.

2.5 Team Members and Volunteers will:

2.5.1 Contribute to the development of online safety policies.

2.5.2 Agree and adhere to the terms on acceptable use of technology and social media, including Phoenix's ICT systems and the internet (appendix 3), and ensuring that People we support follow Phoenix's terms on acceptable use (appendices 1 and 2)

2.5.3 Read and adhere to all the relevant policies including the online safety policy.

2.5.4 Model good practice when using technology and maintain a professional level of conduct in the use of technology.

2.5.5 Embed online safety education in curriculum delivery in education settings and engage People we support in online safety within their homes and the community.

2.5.6 Have an awareness of a range of online safety issues and how they may be experienced by the vulnerable individuals in their care.

2.5.7 Identify online safety concerns and take appropriate action by following the Organisation's safeguarding policies and procedures.

2.5.8 Know when and how to escalate online safety issues.

2.5.9 Take personal responsibility for professional development in this area.

2.5.10 On leaving the Organisation, handover IT equipment (laptop, phones, chargers, DVDs/CD media) and undertake a data handover.

2.6 Team Members managing the technical environment will:

2.6.1 Provide technical support and perspective to the DSLs/DSPs and leadership teams, especially in the development and implementation of appropriate online safety policies/procedures.

2.6.2 Implement appropriate security measures (including password protection and encryption) to ensure that the Organisation's IT infrastructure is secure and not open to misuse or malicious attack.

2.6.3 Ensure that that Phoenix's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.

2.6.4 Block access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files.

2.6.5 Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSLs/DSPs and leadership teams in accordance with the Organisation's safeguarding procedures.

2.6.6 Ensure all organisation equipment when a Team Member leaves is returned to IT and checked, cleansed and suitable audit for re-use as applicable.

2.7 Parents, Carers, and Social Workers will:

2.7.1 Read the Acceptable Use Statement (Appendix 1) and encourage the People we support to adhere to it.

2.7.2 Support the setting in their online safety approaches by discussing online safety issues with the People we support and reinforce appropriate, safe online behaviour at home.

2.7.3 Role model safe and appropriate use of technology and social media.

2.7.4 Identify change in behaviour that could indicate that the Person we support is at risk of harm online.

2.7.5 Seek help and support from the college / school, or other appropriate agencies, if they or the Person we support encounters risks or concerns online.

2.7.6 Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

2.8 Visitors and Volunteers will:

2.8.1 Visitors and Volunteers who use the companies' ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

3. Education and Training

3.1 Our approach

3.1.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating the People we support to take a responsible approach. The education of People we support in online safety/digital literacy is therefore an essential part of our online safety provision.

3.1.2 All People we support, will have access to educational resources such as Project Evolve. This is an educational programme which is based on UKCIS framework "Education for a Connected World" (EFACW). It covers knowledge, skills, behaviours, and attitudes across eight strands of our online lives from early years right through to eighteen. These outcomes or competencies are mapped to age and progressive. The statements guide our Team Members as to the areas they should be discussing with the People we support as they develop their use of online technology

3.1.3 A key aspect of our approach is to help the People we support learn to manage their own digital footprint, including how to:

- use privacy settings to maintain some control over who they are sharing with.
- block people with whom they are not comfortable communicating or sharing with.
- remove content they have shared online; and report content which other people have posted to get it taken down.

3.1.4 In addition, we explore themes such as pornography, consent, and the characteristics of healthy and unhealthy relationships, as appropriate through relationships education and/or relationships and sex education.

3.1.5 Clear boundaries are set for the appropriate use of the internet and digital communications and are discussed with the People we support and Team Members. The People we support are given the opportunity to explore and discuss online safety issues to build a resilience that equips them to manage their own online safety both in and out of Phoenix settings. Positive and responsible technology use is recognised and rewarded. All Team Members receive safeguarding, child/adult protection and, where appropriate, online safety training, in accordance with their roles and responsibilities.

3.1.6 Phoenix is aware that some People we support are considered to be more vulnerable online due to a range of factors.

3.1.7 Phoenix will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable Pupils/Learners and will seek input from specialist Team Members as appropriate, including the Designated Safeguarding Leads, ICT specialists , and external agencies where appropriate.

3.2 Training and Engagement with Team Members

3.2.1 The Organisation will:

3.2.2 Provide and discuss the online safety policy with all Team Members as part of induction.

3.2.3 Provide Child Exploitation Online Protection training on behalf of the National Crime Agency in line with the following CEOP Education Values:

- Safeguarding first - the safety and wellbeing of each child always comes first.
- Approach from the perspective of the child/young person - let them start the conversation. Understand what the online world means to them and explore the positive opportunities it presents, as well as the risks.
- Promote dialogue and understanding - young people are safest when they feel listened to and understood - and know that they can ask trusted adults for help when they need it.
- Empower and enable People we support to know that they have the right to be protected from harm, and to be supported to build knowledge, skills and confidence which will help them identify risk and access support when they need it.
- Never frighten or scare-monger - alarmist education can be risky and ineffective. Avoid shocking or scaring young people, their families, or other professionals.
- Challenge victim blaming attitudes - we all have a responsibility to challenge victim-blaming whenever it arises. CEOP Education helps young people understand that abuse is never the fault of those who have been harmed, and builds their confidence to ask a trusted adult for help when they need it.

3.2.4 Provide up-to-date and appropriate online safety training for all Team Members. This will cover the potential risks posed to vulnerable individuals (e.g., *Content, Contact* and *Conduct, Commercial exploitation*) as well as our professional practice expectations.

3.2.5 Make Team Members aware that organisation systems are monitored, and activity can be traced to individual users; Team Members will be reminded to behave professionally and in accordance with Organisation policies including the Code of Conduct when accessing organisation systems and devices.

3.2.6 Make Team Members aware that their online conduct outside of work, including personal use of social media, could have an impact on their professional role and reputation.

3.2.7 Highlight useful educational resources and tools which Team Members should use, according to the age and ability of those in their care.

3.2.8 Ensure all Team Members are aware of the procedures to follow regarding online safety concerns affecting those they support and Team Members.

4. Reducing Online Risks

4.1.1 Phoenix recognises that the internet is a constantly changing environment with new 'apps', devices, websites, and material emerging at a rapid pace. We will:

4.1.2 Regularly review the methods used to identify, assess, and minimise online risks.

4.1.3 Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in our settings is permitted.

4.1.4 Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

4.1.5 Ensure that all Team Members are encouraged to be vigilant and are aware of the risks of online content, including that which could be accessed through the use of mobile data and external internet sources.

4.1.6 Acknowledge that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a organisation device.

4.1.7 Ensure all are made aware of the Organisation's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments or media which could cause harm, distress, or offence to others. This is clearly outlined in education and training approaches.

4.1.8 To use social media sites which are appropriate for their age and abilities.

4.1.9 How to block and report unwanted communications and report concerns both within the setting and externally.

4.2 Educating Parents and Carers about online safety

4.2.1 Our settings will raise Parent/Carer awareness of online safety in letters or other communications, as appropriate, and in information via our website and social media platforms.

4.2.2 This policy will also be shared with Parents and Carers.

4.2.3 If Parents/Carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head Teacher/Principal/Manager and/or the DSL/DSP.

4.2.4 Concerns or queries about this policy can be raised with any Team Member or the Manager of the setting.

4.3 Use of Mobiles

4.3.1 When working directly with the People we support, Team Members should refrain from using their mobile phones. They should reserve the use of phones until scheduled break times, periods away from the People we support or after they have finished their work. Under no circumstances should personal mobile phones be given to People we support for their use.

4.4 Digital cameras

4.4.1 Phoenix Team Members may be provided with digital cameras, tablets or mobile phones, which are provided strictly for the use of cataloguing and recording the progress, experiences and achievements of the People we support

4.4.2 Under no circumstances should Team Members use their own personal cameras, including mobile phone cameras, to take images of People we support.

4.5 Games Consoles & other Electronic Technology

4.5.1 The use of these technologies can put children, young people and vulnerable adults at risk within and outside the residential or education settings. Some of the dangers they may face include:

- Access to illegal, harmful, or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- Risk of radicalisation.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Online Bullying (cyberbullying).
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy, and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- Risk of addiction on games and online content, impacting mental health and wellbeing

4.5.2 The potential for excessive use which may impact on the social and emotional development and learning of the Person we support.

5. Responding to Online Safety Incidents and Concerns

5.1.1 All Team Members will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, youth produced sexual imagery (sexting), online bullying (cyberbullying) and illegal content.

5.1.2 The Click CEOP reporting button is implemented on our website, providing the People we support with information and a direct reporting route to the CEOP Safety Centre, part of the National Crime Agency.

5.1.3 All Team Members must respect confidentiality and the need to follow the official Organisation safeguarding procedures for reporting concerns.

5.1.4 The organisation requires Team Members, Parents, Carers, and People we support to work in partnership to resolve online safety issues. After any investigations are completed, the Organisation will debrief, identify lessons learnt and implement any policy or curriculum changes as required. If the organisation is unsure how to proceed with an incident or concern, the DSL/DSP will seek advice from the Education and Local Authority Safeguarding Team.

5.1.5 Where there is suspicion, that illegal activity has taken place, the Organisation will contact the Education and Local Authority Safeguarding Team or the Police using 999 if there is immediate danger or risk of harm. If an incident or concern needs to be passed beyond the Organisation environment (for example if other local settings are involved or the public may be at risk), the Organisation will speak with the Police and/or the Local Authority Safeguarding Team first, to ensure that potential investigations are not compromised. Such circumstances must also be shared with the Operations Director responsible for that service.

5.2 Concerns about the welfare of a Person we support.

5.2.1 The DSL/DSP and setting manager will be informed of any online safety incidents involving safeguarding or child protection concerns. The DSL/DSP will record these issues in line with the organisation's child protection policy. The DSL/DSP will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Local Safeguarding Policy, Adult Safeguarding Team, Local Safeguarding Hub procedures.

5.2.2 The organisation will inform Parents, Carers/Social Workers of any incidents or concerns involving the People we support, as and when required.

6. Harmful Online Content

6.1.1 The People we support can come across all sorts of harmful content online, examples of which are outlined in the introduction above. They can come across it by accident, be shown by a friend or family member or they can deliberately search it out.

6.1.2 At Phoenix, we offer direct guidance to People we support who have viewed harmful content based, not only on the nature of the incident, but the individual's age, experience, strengths, vulnerabilities, and circumstances.

6.1.3 In addition, we will ensure that those we support:

- have the opportunity and feel supported to air their views and explore sensitive issues, in a safe and secure environment.
- are supported to explore and manage risks and manage difficult situations online.
- are supported to report and take down content, including helping them to contact providers and/or third parties.
- are aware that what is presented to them online maybe biased, inaccurate, manipulated, or misleading and they should consider where the information/images are coming from.
- have access to emotional and psychological support; and know where they can go to access advice, guidance, support, and resources in relation to online matters including Childline and CEOP.

6.2 Online pornography

6.2.1 Legal adult pornography is readily available online. Many teenagers will at some point seek out pornography because of adolescent curiosity and most are unlikely to suffer any long-term negative effects. However, there is growing concern that children and young people who routinely access pornography are at an increased risk of:

- normalisation of extreme or risky sexual acts, making them more likely to engage in harmful sexual activity.
- developing discriminatory attitudes, perceiving people (particularly girls and women) as sex objects, rather than caring partners. struggling to engage in or enjoy real-life relationships or sexual activity, as pornography has created unrealistic expectations.
- an unhealthy preoccupation with sex, which can interfere with other aspects of their lives.

6.2.2 As of 25 July 2025, platforms have a legal duty to protect children online. Platforms are now required to use highly effective age assurance to prevent children from accessing pornography, or content which encourages self-harm, suicide or eating disorder content.

6.2.3 Platforms must also prevent children from accessing other harmful and age-inappropriate content such as bullying, hateful content and content which encourages dangerous stunts or ingesting dangerous substances. Platforms must also provide parents and children with clear and accessible ways to report problems online when they do arise.

6.2.4 For more information and advice visit:

- Internet Matters - Online pornography resources
- https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer
- Childnet International - Online Pornography
- NSPCC - Online porn

6.3 Violent content and gaming

6.3.1 Some adult games, especially those which involve players talking to others can expose children and young people to scenes that:

- feature extreme violence, warfare, and criminal activity.
- show explicit sexual acts, which may glamorise rape and assault.
- use racist, homophobic, or sexist language and feature swearing.
- depict certain groups, such as women, in derogatory ways.

6.3.2 Although Parents/Carers and professionals will have a view on whether a Person we support is mature enough to play these games, they can be upset or start to normalise violent and aggressive behaviour and/or adopt beliefs associated with the character or game they play.

6.3.3 It is also important to remember that children and vulnerable adults can be groomed or bullied through games and introduced to other content and platforms. In extreme cases, some children, and young adults experience gaming addiction.

6.3.4 Within Phoenix settings, access to age-appropriate games is closely monitored by all Team Members.

6.3.5 For more information and advice visit:

- Childnet International - Gaming
- Internet Matters -Online gaming - The risks
- NSPCC – Online games

6.4 Self-harm and pro-suicide sites

6.4.1 There are many apps, websites, forums, and online chatrooms that work to support mental health. However, there are blogs, forums and websites that can reinforce harmful offline behaviours and encourage self-harm and promote suicide.

6.4.2 The reasons People we support might visit sites like these can be complex, often indicating broader emotional and well-being issues.

6.5 Eating disorder sites

6.5.1 The terms “pro-anorexia”, or “pro-ana”, and “pro-bulimia”, or “pro-mia”, refer to content, usually online, that promotes the harmful behaviour and mindset that forms part of some eating disorders. The sites and social media where such content is found often say or imply that this behaviour is a lifestyle choice, rather than symptoms of an illness.

6.5.2 There is an assumption that people who post pro-ana, pro-mia, or “thinspiration” content are being deliberately malicious, are fully aware that they are misrepresenting symptoms as lifestyle choices, and consciously want to encourage people to develop or continue to have eating disorders. But this is often not the case, as many of the people who post this content are suffering from eating disorders themselves.

6.6 Radicalisation and extremism

6.6.1 Extremist groups often target children and susceptible adults via the internet and social media. Groups can easily share propaganda via online platforms like Facebook, YouTube, and Instagram.

6.6.2 Online radicalisation and extremism can pose a significant threat to the well-being and safety of the People we support, which may involve:

- being groomed online or in person.
- exposure to violent/upsetting material and other inappropriate information.
- psychological manipulation.
- isolation from friends and family.
- sexual and commercial exploitation.
- encouraging children and young people to act in a way that puts them at risk of physical harm or death. Phoenix acknowledges its duty under section 26 of the Counterterrorism and Security Act 2015, (the CTSA 2015) to have “due regard to the need to prevent people from being drawn into terrorism”. This duty is known as the Prevent duty.

6.6.3 In meeting our obligations, we:

- Assess the risk of the People we support being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology.
- Protect the People we support from being drawn into terrorism, by having robust safeguarding policies in place to identify children and young people at risk, and intervene, as appropriate.

- Educate the People we support with a programme which promotes the spiritual, moral, cultural, mental, and physical development and prepares them for the opportunities, responsibilities, and experiences of life. We also place a strong emphasis on the fundamental British values of democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs.

- Ensure that the People we support are safe from terrorist and extremist material when accessing the internet on our sites, including by establishing appropriate levels of filtering and monitoring.

6.6.4 Identification, assessment, and management of such risks form an integral part of our referral and admissions procedures, and any concerns would be recorded and addressed, in accordance with national and local guidance.

6.6.5 For further information, see our Safeguarding and Child / Adult Protection Policies

6.6.6 For more information and advice visit:

- Internet Matters - Tackling radicalisation facts & advice.

- Educate Against Hate - This website provides practical advice, support, and resources to protect children and young people from extremism and radicalisation.

7. Harmful contact online

7.1 Online grooming and sexual abuse

7.1.1 Sexual grooming is a process through which an offender seeks to build trust with a child for the purpose of sexually abusing them. Grooming can be facilitated by technology and most instances of grooming now contain an online component. Offenders build and exploit a trusting relationship with the child and use that trust to exercise manipulation, coercion, and control.

7.1.2 The following examples illustrate the range of techniques offenders use (not an exhaustive list):

- Bribery – offering rewards and gifts.
- Emotional blackmail.
- Flattery.
- Offering and providing emotional support.
- Persistent pressure.
- Pretending it is a game such as truth or dare.
- Pretending to be someone they are not, such as another child.
- Threats.

7.1.3 Even though a child may never meet the offender face-to-face, children forced, tricked, or persuaded to participate in online abuse may be left with long-term trauma from the experience and can suffer just as much harm as those abused by an offender in the 'offline' world.

7.1.4 If you become aware of a situation in which a child may have been groomed and/or sexually abused online, you must inform the Setting Manager/ Headteacher/ Principal and DSL/ DSP as a matter of urgency.

7.1.5 For more information and advice visit:

- Childline - Online grooming
- Childnet International – Online grooming
- Internet Matters – Deal with it

7.2 Online bullying

7.2.1 Online bullying (sometimes called cyberbullying) is bullying that happens online via apps, online games, social networks, websites and photo, text, and video messaging. It can happen when using any device and takes many forms:

- abusive or threatening texts, emails, or messages.
- posting abusive comments on social media sites.

- modifying and/or sharing humiliating videos or photos of someone else.
- stealing someone's online identity.
- spreading rumours online.
- trolling – sending someone menacing or upsetting messages through social networks, chatrooms, or games.
- developing hate sites about another person prank calls or messages.
- group bullying or exclusion online.
- anonymous messaging.
- encouraging a child or vulnerable adult to self-harm.

7.3 Harmful conduct online

7.3.1 Many children share personal content online including:

- photos and videos of themselves, their friends, and things they like.
- videos and live streams of themselves talking to camera, performing, or gaming.
- blogs
- comments on their own and other people's uploaded content

7.4 Financially Motivated Sexual Extortion

7.4.1 Financially Motivated Sexual Extortion (FMSE) is a type of online blackmail, where victims are forced into paying money or meeting another financial demand after an offender has threatened to release nude or semi-nude photos or videos of them. Where the victim is under 18, it is also a form of child sexual abuse.

7.4.2 Victims report being:

- Contacted by an online account they do not know.
- Quickly engaged in sexually explicit communications.
- Encouraged to chat on an encrypted platform.
- Manipulated or pressured into taking nude or semi-nude photos or videos.
- Sent nude or semi-nude images of themselves, that have been digitally manipulated.
- Blackmailed into sending money or meeting another financial demand e.g. gift cards

7.5 Child Sexual Abuse Material

7.5.1 Child sexual abuse material is when a nude or semi-nude image of a child is shared. The image could be self-created by a child, created using AI technology or other apps or by another child or adult. . Adults sometimes refer to this as 'sexting' which can include sending sexually suggestive comments. However, children use many other terms for this behaviour such as nudes, which includes semi-nude images. It is important to remember this when talking to children.

7.5.2 There are many reasons why a child might share a nude or semi-nude image or video. Some situations are riskier than others.

7.5.3 Across the UK it is illegal for anyone, including a child, to make, possess or share an indecent image of someone under 18 years of age.

7.5.4 If a child has been pressured, manipulated, or coerced into sharing an explicit image of themselves and/or you become aware of a situation in which a child has shared a youth-produced sexual image with an adult you must inform the Designated Safeguarding Lead (DSL/DSP) as a matter of utmost urgency.

7.5.5 Be aware that if a child has been groomed, they may not realise they are being abused.

- For further information and advice see Department for Digital, Culture, Media & Sport, and UK Council for Internet Safety (2020).
- 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'.
- Childnet International - Sexting Internet Matters - Dealing with sexting NSPCC - Sexting and sending nudes.

7.6 Managing Incidents Involving Sexual Images

7.6.1 The production, possession, and distribution of sexual images involving individuals under the age of 18 is a criminal offence under UK law, regardless of whether the individuals involved consented.

7.6.2 For vulnerable adults, while the sharing of sexual images may not be illegal, their circumstances may require heightened safeguarding measures to protect their best interests, dignity, and well-being.

7.7 Team Member Responsibilities

7.7.1 When an incident involving the sharing of sexual images (including nudes or semi-nudes) comes to light Team Members must:

- Report the incident without delay to the Designated Safeguarding Lead (DSL/P) using the setting's established safeguarding procedures. Timely reporting is essential to ensure appropriate support and risk management.
- Respond to those involved calmly and without judgment. Avoid language or behaviour that could be perceived as blaming or shaming. The goal is to create a safe space for disclosure and support.

- Do not delete or forward any images. Secure devices or evidence, if necessary, but avoid viewing or sharing the content. This helps preserve the integrity of any potential investigation.

7.7.2 Team Members and the DSL/P must ensure that the Person we support's voice is heard throughout the process, and that they are supported to understand what has happened, what steps may follow, and what choices they have moving forward.

7.8 Designated Safeguarding Lead (DSL/P) Responsibilities

7.8.1 Upon receiving a report, the DSL/P must record the incident thoroughly, including:

- Date and time of report
- Individuals involved
- Nature of the image(s)
- Actions taken
- Rationale for decisions made
- Any advice sought or received.

7.8.2 Evaluate the incident by considering:

- Age differences between those involved, especially if one party is significantly older.
- Evidence of coercion, manipulation, or external pressure.
- Whether the child or adult is particularly vulnerable due to other safeguarding concerns.
- The explicit nature of the image, whether it is sexually graphic or suggestive.
- Whether the image has been widely shared or remains contained.
- Previous incidents, patterns of behaviour or recurring concerns.

7.9 Escalation Protocol

7.9.1 If any of the above risk factors are present, the DSL/P must escalate the incident. This may include:

- Reporting to the Police or CEOP. https://www.ceop.police.uk/ceop-reporting/
- Contacting Children's Services or Adult Safeguarding Teams
- Seeking advice from external safeguarding bodies

7.9.2 If no significant risk factors are identified, the incident may be managed internally, however:

- It must still be fully documented
- Support must be offered to all parties involved
- Preventative education or interventions should be considered

7.10 Support and Advice:

7.10.1 For further guidance, Team Members may contact the Professionals Online Safety Helpline at 0844 381 4772.

7.10.2 UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges

7.11 Safe use of digital images

7.11.1 The term "images" refers to photographs (digital and film), 'video', DVD, and webcam recordings.

7.11.2 Team Members and the People we support need to be aware of the risks and pressures associated with sharing images and publishing digital images on the internet.

7.11.3 Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

7.11.4 Phoenix will inform and educate users about these risks and pressures and will implement policies to reduce the likelihood of any potential for harm.

- Images published on our website, in our brochure, newsletter, or elsewhere, including those released to local and national media, that include People we support and Team Members will be selected carefully and will comply with good practice guidance on the use of such images.
- Permission must be obtained from the Person we support, their Parents/Carers, or other responsible adult (e.g., social worker) before images (and positive examples of their work) are recorded or distributed in any form
- Where a Person we support does not have capacity to give consent, Parents/ Carers cannot give consent. If an image of a child is to be used without their consent, there must be evidence to show that it was in the best interest of the child.

7.11.5 A Person we support must be asked if they are happy (if they consent) for their image to be recorded each and every time a photograph or 'video' is to be created. They should be informed that they can choose whether or not to have their image recorded, how much or little they would like particular images to be shared; and they can change their mind at any time before, during or after the images have been taken.

7.11.6 Written permission from a child, their Parents/Carers or other responsible adult (e.g., social worker) must be obtained before images of children (and positive examples of their work) are recorded or distributed in any form. Written permission must also be obtained from Team Members, as appropriate.

7.11.7 Similarly, you must get the permission of anyone in an image, including Team Members or those who are not part of a crowd and easily recognisable.

7.11.8 Team Members must only use organisation equipment to take or store images of People we support.

7.11.9 Care should be taken when taking digital/video images that People we support and Team Members are appropriately dressed and are not participating in activities that might bring the individuals or Phoenix into disrepute.

7.11.10 It is the responsibility of those using images, to check that consent forms are current, and the Person we support or Team Member is still in agreement. Senior Team Members must also check that there are no outstanding concerns or issues associated with the individual, which would make the use of their image inappropriate.

7.11.11 All images created by Team Members in their capacity as a Team Member, are the property of Phoenix and copyright rests with Phoenix.

7.11.12 Images taken by authorised external photographers (see below) will be purchased outright as part of the package for unlimited use and thus remain the property of Phoenix. Images taken by any Person we support are the property of the Person we support and relevant consents must be obtained before using the images.

7.11.13 The hiring of authorised external photographers will be done through Phoenix. All external photographers will be briefed on the nature of our business and will be obliged to abide by our safeguarding and child protection procedures. All relevant checks will be conducted, in accordance with our Child /Adult Protection Policy.

7.11.14 All images of People we support and Team Members must be stored securely on a password-protected device. Any sharing of images must comply with the General Data Protection Regulation (GDPR) and Data Protection Act 2018

7.11.15 Full names and/or personal details of People we support and Team Members will not be published anywhere on our website, in our brochure, newsletter or elsewhere, particularly in association with photographs.

7.11.16 Given the potential for misuse, children are not permitted to use personal digital cameras or other photographic equipment without the express permission of the setting manager.

7.11.17 Photographs can be taken with the full knowledge and consent of the person concerned, but children must not use, share or distribute images of Team Members, People we support or visitors under any circumstances.

7.11.18 When using digital images, Team Members, should inform and educate the People we support about the risks associated with the taking, use, sharing, publication and distribution of images.

7.11.19 In accordance with guidance from the Information Commissioner's Office, Parents/Carers are welcome to take videos and digital images of their children at Phoenix events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should Parents/Carers comment on any activities involving other children or People we support in the digital/video images.

8. Responding to incidents of misuse

8.1 Behaviour support plans and risk assessments

8.1.1 Where a Person we support has been involved in an online safety or multi-media incident, new information will be recorded, as appropriate. Relevant information will be communicated to other Team Members, as soon as reasonably possible, and the individual risk assessment and/or behaviour support plan will normally be reviewed and redistributed (where appropriate) within 72 hours.

8.1.2 All relevant Team Members are obliged to familiarise themselves with the current risk assessment and behaviour support plan, for every person they are likely to have responsibility for educating, engaging, supporting, or supervising. All risk assessments and support plans are shared with People we support to enable them to develop the knowledge, understanding and skills necessary to manage their own behaviour effectively.

8.2 Team Member Misuse

8.2.1 Any complaint about Team Member misuse will be referred to the DSL/DSP. Appropriate action will be taken in accordance with the Team Member Code of Conduct.

9. Useful Links

9.1 Local Support and Guidance

9.1.1 National Links and Resources

- Action Fraud: www.actionfraud.police.uk
- www.thinkuknow.co.uk
- www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for colleges: www.360safe.org.uk
- EE Digital Living resources - for colleges and Parents and Carers.
- NWG and UK Safer Internet Centre leaflet: Online: On guard - A Guide to Becoming a Safer Parent Online