ONLINE AND E-SAFETY POLICY

Contents

United Learning
The best in everyone™

■ Ambition ■ Confidence ■ Creativity ■ Respect ■ Enthusiasm ■ Determination

Introduction

United Learning believes that the safe use of information and communication technologies brings great benefits. Recognising online safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

Creating an Online Safety Ethos

Aims and policy scope

- North Oxfordshire Academy believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones, or games consoles.

- North Oxfordshire Academy identifies that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

- North Oxfordshire Academy has a duty to provide the school community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff, and enhance the school's management functions. North Oxfordshire Academy also identifies that with this there is a clear duty to ensure that children are protected from potential harm online.

- The purpose of North Oxfordshire Academy online safety policy is to: o Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that North Oxfordshire Academy is a safe and secure environment.
    - Safeguard and protect all members of North Oxfordshire Academy community online.
    - Raise awareness with all members of North Oxfordshire Academy community regarding the potential risks as well as benefits of technology.
    - To enable all staff to work safely and responsibly to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

- This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop or mobile phone.

- This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including

computing, Personal Social Health and Education (PSHE), Citizenship and Sex and Relationships education (SRE).

Writing and reviewing the online safety policy

- North Oxfordshire Academy online safety policy has been written by the school, involving staff, pupils and parents/carers, building on the United Learning online safety policy template with specialist advice and input as required.

- The policy has been approved and agreed by the Leadership/Management Team and governing body.

- The school has appointed a member of the Governing Body to take lead responsibility for online safety (eSafety).

- The school has appointed a member of the leadership team as the online safety lead.

- The school's online safety (e–Safety) Policy and its implementation will be reviewed at least annually or sooner if required.

The School Online safety (e-Safety) Coordinator is D Jeffs

The School Designated Safeguarding Lead (DSL) is Sophie McFarlane (*If different to online safety lead*)

The School Online safety (e-Safety) lead for the Governing Body is Victoria Espley

Policy approved by Head Teacher: Date: 06/02/2023

Policy approved by Governing Body (Chair of Governors) Date: 06.02.2023

The date for the next policy review is February 2024

Key responsibilities of the community

- Developing, owning, and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.

- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.

- Supporting the online safety (e-Safety) lead in the development of an online safety culture within the setting.

- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.

- To ensure that suitable, age-appropriate, and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored.

- Ensuring all members of staff receive regular, up-to-date, and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.

- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.

Making appropriate resources available to support the development of an online safety culture.

- Taking responsibility for online safety incidents and liaising with external agencies as appropriate.

- Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.

- Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local, and national support.

- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.

- To work with and support technical staff in monitoring the safety and security of school systems and networks.

- To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.

- To ensure that the Designated Safeguarding Lead (DSL) works in partnership with the online safety (eSafety) lead.

Key responsibilities of the designated safeguarding/online safety lead are:

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.

- Keeping up to date with current research, legislation, and trends.

- Coordinating participation in local and national events to promote positive online behaviour, e.g., Safer Internet Day.

- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.

- Work with the school/setting lead for data protection and data security to ensure that practice is in line with legislation.

- Maintaining an online safety incident/action log to record incidents and actions taken as part of the school's safeguarding recording structures and mechanisms by using the *child protection/safeguarding files*

- Monitor Internet filtering reports to identify behaviour which might indicate safeguarding issues or inappropriate behaviours. Update safeguarding log or e-safety incident log as appropriate.

- Monitor the school/settings online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school management team, Governing Body, and other agencies as appropriate.

- Liaising with the local authority and other local and national bodies as appropriate.

United Learning
The best in everyone™ ▪ Ambition ▪ Confidence ▪ Creativity ▪ Respect ▪ Enthusiasm ▪ Determination

-
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Meet regularly with the governor/board/committee member with a lead responsibility for online safety

Key responsibilities of staff are:

- Contributing to the development of online safety policies.
- Reading and signing the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school/setting systems and data.
- Having an awareness of online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by working with the designated safeguarding lead.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.

Additional responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety lead and DSL.
- Ensuring that the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead and DSL.

- Report any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded on the e Safety Incident Log, and appropriate action is taken as advised.

- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.

- Report any breaches and liaise with United Learning Technology Team (or other local or national bodies) as appropriate on technical infrastructure issues.

- Configure internet filters to generate regular safeguarding reports, as determined by e-safety lead, pastoral leads, and DSL, and send to appropriate staff.

  Providing technical support and perspective to the online safety lead and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.

- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.

- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.

- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

Key responsibilities of children and young people are:

- Contributing to the development of online safety policies.

- Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them.

- Respecting the feelings and rights of others both on and offline.

- Seeking help from a trusted adult if things go wrong and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability, and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.

- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

- Assessing the personal risks of using any particular technology and behaving safely and responsibly to limit those risks.

Key responsibilities of parents and carers are:

- Reading the school/setting Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.

United Learning
The best in everyone™   ■ Ambition   ■ Confidence   ■ Creativity   ■ Respect   ■ Enthusiasm   ■ Determination

-
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.

- Role modelling safe and appropriate uses of new and emerging technology.

- Identifying changes in behaviour that could indicate that their child is at risk of harm online.

- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

- Contributing to the development of the school/setting online safety policies.

- Using school systems, such as learning platforms, and other network resources, safely and appropriately.

- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Online Communication and Safer Use of Technology

Managing the school/setting website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.

- The contact details on the website will be the school address, email, and telephone number. Staff or pupils' personal information will not be published.

- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

- The school website will comply with United Learning's and the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

- The school will post information about safeguarding, including online safety on the school website, or link to the resources hosted by United Learning.

- The administrator account for the school website will be safeguarded with an appropriately strong password.

- Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)

- Pupils' work will only be published with their permission or that of their parents/carers.

Publishing images and videos online

- The school will ensure that all images are used in accordance with the school image use policy.

- In line with the school's image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

- Any images, videos or music posted online will comply with the intellectual property rights and copyright

Managing email

- Pupils may only use school/setting provided email accounts for educational purposes.
- All members of staff are provided with a specific school/setting email address to use for any official communication.
- The use of personal email addresses by staff for any official school/setting business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.
- Members of the school community must immediately tell a designated member of staff if they receive offensive communication, and this should be recorded in the school online safety incident log.

  Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- Caution should be taken on opening emails with attachments or clicking on links within; being conscious of the risks from malware.
- Whole -class or group email addresses may be used for communication outside of the school.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The school will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

Official videoconferencing and webcam use

- All videoconferencing equipment in the classroom will be switched off when not in use and where appropriate, not set to auto answer.
- The equipment will be kept securely and if necessary locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.

United Learning
The best in everyone™

■ Ambition ■ Confidence ■ Creativity ■ Respect ■ Enthusiasm ■ Determination

-
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.

- Staff will ensure that external videoconference are suitably risk assessed and that accounts and systems used to access events are appropriately safe and secure.

- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

Users

- Pupils will ask permission from a teacher before making or answering a videoconference call or message.

- Videoconferencing will be supervised appropriately for the pupils' age and ability. (Schools should list how this will be enforced and achieved).

- Parents and carers consent will be obtained prior to children taking part in videoconferences.

- Video conferencing will take place via official and approved communication channels following a robust risk assessment.

Content

- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.

- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third-party intellectual property rights.

- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site, the school will check that they are delivering material that is appropriate for the class.

Remote Teaching and Learning

Due to the current pandemic, teachers are teaching remotely, and students are logging into virtual lessons from home. The measures teachers at North Oxfordshire Academy are taking to ensure there are no safeguarding issues are:

- When teaching a virtual lesson, the teacher will record the lesson and this message will be shared with students.
- Recordings of a lesson can be used to deal with behaviour issues during virtual lessons.
- Teaching staff will mute students on Teams before and after the lesson.

- Teaching staff will make sure that if they are on camera, that they have a professional background.
- Students are to log on to Teams with their school email address.
- Students have the Student Code of Conduct available to them so they can read and understand what is expected of them during a live lesson.
- Students will only use the group chat to ask relevant questions. If they type anything inappropriate, teachers follow the behaviour policy of move and remove. Teachers can remove a student from the team lesson, mute the student and communicate any poor behaviour online to the relevant Learning Manager.

Appropriate and safe classroom use of the internet and associated devices

- The school's internet access will be designed to enhance and extend education.

- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.

- Pupils will use age and ability appropriate tools to search the Internet for content. This is enforced by Safe Search on Google and Bing, we also use **Senso.Cloud** and our internet filtering through **fortigate** will categorise and block inappropriate sites.

  Internet use is a key feature of educational access, and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.

- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.

- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use are essential.
    - Supervision of pupils is appropriate to their age and ability by being appropriately supervised when using technology, according to their ability and understanding.

- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place. All internet traffic goes via the Academy's internet filtering and all Academy Laptops, and some tablets have Impero installed.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation.

- The school will use age-appropriate search tools enforced by Safe Search and the FortiGate filtering and Impero will monitor and block inappropriate content. This was decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.

- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

-
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole school/setting requirement across the curriculum.

- Members of staff will always evaluate websites, tools, and apps fully before use in the classroom or recommending for use at home.

Management of school learning platforms/portals/gateways (LP)

SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.

- Pupils/staff will be advised about acceptable conduct and use when using the LP.

- Only members of the current pupil, parent/carers and staff community will have access to the LP.

- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

- When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

- Any concerns about content on the LP may be recorded and dealt with in the following ways:
    - a) The user will be asked to remove any material deemed to be inappropriate or offensive.
    - b) The material will be removed by the site administrator if the user does not comply.
    - c) Access to the LP for the user may be suspended.
    - d) The user will need to discuss the issues with a member of leadership before reinstatement. e) A pupil's parent/carer may be informed.

- A visitor may be invited onto the LP by a member of the leadership team. In this instance there may be an agreed focus or a limited time slot.

- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

Policy Decisions

Reducing online risks

- North Oxfordshire Academy is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites, and material emerging at a rapid pace.

- Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.

- The school will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. Schools should include appropriate details about the systems in place.

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device.

- The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.

- Methods to identify, assess and minimise online risks will be reviewed regularly by the school's leadership team.

- Filtering decisions, internet access and device use by pupils and staff will be reviewed regularly by the school's leadership team.

Internet use throughout the wider school/setting community

- The school will liaise with United Learning and local feeder schools to establish a common approach to online safety (e–Safety).

- The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site.

Authorising internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

- All staff, pupils and visitors will read and sign the School Acceptable Use Policy before using any school ICT resources.

- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.

-
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.

  When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

Engagement Approaches

Engagement and education of children and young people

- An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.

- Education about safe and responsible use will precede internet access.

- Pupil's input will be sought when writing and developing school online safety policies and practices.

- Pupils will be supported in reading and understanding the school Acceptable Use Policy in a way which suits their age and ability.

- All users will be informed that network and Internet use will be monitored.

- Pupil instruction regarding responsible and safe use will precede Internet access.

- Online safety (e-Safety) will be included in the PSHE and Computing programmes of study covering both safe school and home use.

- Online safety (e-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.

- The pupil Acceptable Use expectations and Posters will be posted in all rooms with Internet access.

- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.

- External support will be used to complement and support the school's internal online safety (e-Safety) education approaches.

- The school will reward positive use of technology by pupils.

- The school will implement peer education to develop online safety as appropriate to the needs of the pupils.

Engagement and education of children and young people who are considered to be vulnerable

☐ North Oxfordshire Academy is aware that some children may be considered to be more vulnerable online due to a range of factors and will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g., SENCO).

-

Engagement and education of staff

- The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of school safeguarding practice.

- To protect all staff and pupils, the school will implement Acceptable Use Policies which highlights appropriate online conduct and communication.

  Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.

- Members of staff with a responsibility for managing filtering systems or monitoring ICT use will be supervised by the leadership team and will have clear procedures for reporting issues or concerns.

- The school will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.

- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal, or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Engagement and education of parents and carers

- North Oxfordshire Academy recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.

- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g., parent evenings, transition events, fetes, and sports days.

- Parents will be requested to read online safety information as part of the Home School Agreement.

- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.

- Information and guidance for parents on online safety will be made available to parents in a variety of formats.

- Parents will be encouraged to role model positive behaviour for their children online.

-

Responding to Online Incidents and Concerns

- All members of the school/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc.).

- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.

- The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to the United Learning Designated Safeguarding Officer and relevant agencies in line with the Local Safeguarding Children Board thresholds and procedures.

- Complaints about Internet misuse will be dealt with under the school's complaints procedure.

- Complaints about online bullying will be dealt with under the school's anti-bullying policy and procedure

  Any complaint about staff misuse will be referred to the head teacher

- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

- Pupils, parents, and staff will be informed of the school's complaints procedure.

- Staff will be informed of the complaints and whistleblowing procedure.

- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

- The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.

- The school will inform parents/carers of any incidents of concern as and when required.

- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.

- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Local Education Safeguards Team or Local Police via 999 if there is immediate danger or risk of harm.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to United Learning Technology Team and Local Police.

-
  - If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the United Learning Lead Safeguarding Officer or Local Education Safeguarding Team.

  - If an incident of concern needs to be passed beyond the school, then the concern will be escalated to the Local Education Safeguarding Team to communicate to other schools/settings in area.

  - Parents and children will need to work in partnership with the school to resolve issues.

Appendix A Procedures for Responding to Specific Online Incidents or Concerns

The following content is provided to enable schools and education settings to make appropriate safeguarding decisions reading online safety concerns and has been written by the Kent e-Safety Strategy Group with input from specialist services and teams. This content is not exhaustive and cannot cover every eventually so professional judgement and support from appropriate agencies such as the United Learning Safeguarding Team, Police and Children's Social Care is encouraged.

Some settings may not feel that these sections are relevant due to the age and ability of children; however, it is recommended that designated safeguarding leads ensure that their settings safeguarding policies and procedures are robust and are applicable for a range of safeguarding issues should they occur.

Some schools and settings will wish to place these sections within existing safeguarding and child protection policies and procedures rather than the online safety policy or within other appropriate policies and procedures. Other settings will prefer to keep this content as reference material for Designated Safeguarding Leads.

Responding to concerns regarding Self-Generated Indecent Images of Children (SGIIOC or "Sexting")

Discussion:

Self-Generated Indecent Images of Children (SGIIOC or "Sexting") can be defined as images or videos generated by children under the age of 18 that are of a sexual nature or are considered to be indecent. These images may be shared between children and young people and/or adults via a mobile phone, webcam, handheld device, or website. Children and young people will always look to push the boundaries, especially when they go through puberty and are an age where they are more sexually and socially aware. Children typically do not use the term "sexting", usually referring to the images as "selfies" and may decide to send such pictures or videos for many reasons. For younger children (early years and primary school aged) indecent images or videos may be taken or shared out of curiosity or naivety and for older children, indecent images may be taken or shared as a response to peer pressure, cyberbullying, sexual exploration, impulsive behaviour, "flirting" or even exploitation due to blackmail from a friend, partner, or other on or offline contact. Often children and young people and indeed adults are unaware of the social, psychological, and even criminal consequences of sharing such images and videos.

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 an indecent image, advertise indecent images, and possess an indecent image or possess an indecent image with the intention of distribution. This applies even if the images are sent or shared by someone under the age of 18 with "consent". "Sexts" may be viewed as police evidence, and it is essential than schools secure devices and seek advice immediately when dealing with concerns.

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.'

www.ceop.police.uk/Documents/ceopdocs/externaldocs/ACPO_Lead_position_on_Self_Taken_Images.pdf

It should be noted that prosecution of children for sharing indecent images for a first offence is rare. The decision to criminalise children and young people for sending these kinds of images will need to be considered and made on a case-by-case basis, however where possible the intention should not be to criminalise children. Wider vulnerability considerations for all of those involved should always be made and education and safeguarding approaches must always be implemented.

There can also be huge emotional and reputation damage that can come from having intimate photos forwarded to others or shared online. These consequences can include isolation, bullying, low self-esteem, loss of control, creating of a negative "digital footprint" or online reputation, harassment, mental health difficulties, self-harm, suicide and increased risk of child sexual exploitation. Schools and settings will also want to take as many preventative measures as they can to educate young people about the risks and to support them in maintaining a healthy digital footprint.

It is essential that schools and settings handle 'sexting' incidents as carefully as possible and offer support to all parties involved whilst abiding by the law and do not compromise police investigations. Schools and education settings should access and consider the guidance as set out in "'Sexting' in schools: advice and support around self-generated images. What to do and how to handle it" which can be downloaded from the Kelsi website: http://www.kelsi.org.uk/support-for-children-and-young-people/child-protectionandsafeguarding/esafety

The following statements may enable schools and settings to consider how best to respond to concerns relating to 'sexting':

- What is the age of the child(ren) involved? ○ If under 13 then a consultation/referral to Children's Social Care should be made.
    - ○ If an adult (over 18) is involved, then consider using the KSCB CSE toolkit.
- Is there any contextual information to help inform decision making? ○ E.g., are the children involved in a relationship and if so is the relationship appropriate?
    - ○ Is this age-appropriate experimentation, natural curiosity, or possible exploitation?
- Is the school or other agencies (e.g. Police or social care) aware of any vulnerability for the children(s) involved?
    - ○ E.g., special education needs, emotional needs, children in care, youth offending?
- Are there any other risks or concerns known by the school or other agencies which may influence decisions or judgements about the safety and wellbeing of the child(ren) involved?
    - ○ E.g., family situation, children at risk of sexual exploitation?

United Learning
The best in everyone™

■ Ambition ■ Confidence ■ Creativity ■ Respect ■ Enthusiasm ■ Determination

-
- How were the school made aware of the image? ○ E.g. did a child disclose about receiving, sending or sharing an image themselves or was the concern raised by another pupil or member of the school community?
- What sort of image is it?
  - Is the image potentially illegal or is it inappropriate?

  Does the child(ren) know who has accessed the image?
  - E.g., was it sent to a known peer (e.g., boyfriend or girlfriend) or an unknown adult? ○ Do they know where the image has been shared?
  - Has it been shared online or sent to another child/person?
- How widely has the image been shared? ○ E.g., just to one other child or to an unknown number of children/adults?
- Are there other children/pupils involved? ○ If so, who are they and are there any safeguarding concerns? ○ What are their views/perceptions on the issue?
- What apps, services or devices are involved (if appropriate)? ○ Some apps and devices may automatically store, backup or delete images which can influence evidence gathering.
- Is the image on a school device or a personal device? ○ Is the device secured?
     - Schools and settings must NOT print/copy etc. images suspected to be indecent – the device should be secured until advice can be obtained.
- Does the child need immediate support and or protection? ○ What is the impact on the child? ○ What can the school put in place to support them?
- Are other schools/settings involved? ○ Does the relevant Designated Safeguarding Lead need to be identified and contacted?
- Is this a first incident or has the child(ren) been involved in sexting concern before? ○ If so, what action was taken and does this possibly increase concerns for offending behaviour? □ Are the school child protection and safeguarding policies and practices being followed? ○ for example, is a member of the child protection team on hand and is their advice and support available?

The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff, and parents/carers.

- North Oxfordshire Academy views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead (name and role).
- If the school are made aware of incident involving indecent images of a child, the school will:
- Act in accordance with the school's child protection and safeguarding policy and the relevant Local Safeguarding Child Boards procedures.

United Learning
The best in everyone™   ■ Ambition   ■ Confidence   ■ Creativity   ■ Respect   ■ Enthusiasm   ■ Determination

- Immediately notify the designated safeguarding lead.

- Store the device securely.

- Carry out a risk assessment in relation to the children(s) involved.

- Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)

- Make a referral to children's social care and/or the police (as needed/appropriate). Put the necessary safeguards in place for children e.g., offer counselling support and immediate protection and offer appropriate pastoral support for those involved.

-
-
  Inform parents/carers about the incident and how it is being managed.
  Implement appropriate sanctions in accordance with the school's behaviour policy but taking care not to further traumatise victims where possible.

- Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.

- The school will not view the image unless there is a clear need or reason to do so.

- The school will not send, share or save indecent images of children and will not allow or request children to do so.

- If an indecent image has been taken or shared on the school/settings network or devices, then the school will take action to block access to all users and isolate the image.

- The school will need to involve or consult the police if images are considered to be illegal. The school will act regarding indecent images, regardless of the use of school/setting equipment or personal equipment, both on and off the premises.

- The school will follow the guidance (including the decision-making flow chart and risk assessment template) as set out in "'Sexting' in schools: advice and support around self-generated images. What to do and how to handle it".

- The school will ensure that all members of the community are aware of sources of support.

Responding to concerns regarding Online Child Sexual Abuse

Discussion:

Online child sexual abuse within this policy context is specifically defined as when children are sexually abused or exploited via the use of technology and the internet. Typically, this is referred to as "online grooming" however this term can sometimes be considered to be too narrow when considering online child sexual abuse as using the term "grooming" may imply that the behaviour has taken place over a period whilst an offender has built a relationship and gained the trust of their victim. Whilst this longer-term process still occurs, current trends identified nationally (CEOP/NCA) and locally would suggest that the period of engagement between offender and victim can in many cases be extremely brief. In 2015, CEOP identified that the objectives of online child sexual abuse have evolved and can lead to a range of offending outcomes, such as deceiving children into producing indecent images of themselves or engaging in sexual chat or sexual activity over webcam. Online child sexual abuse can also result in offline offending such as meetings between an adult and a child for sexual purposes following online engagement.

OSCE can also be perpetrated by young people themselves and these issues should be viewed and responded to in line with the Local Safeguarding Children Board procedure for children who display harmful behaviours

Online child sexual abuse can also link in with Child Sexual Exploitation

•

Schools must be aware of and understand the law regarding the online sexual abuse and exploitation of children. Specifically, (but not limited to):

The Sexual Offences Act 2003 – Section 15. Meeting a child following sexual grooming.

The Sexual Offences Act 2003 – Section 8. Causing or inciting a child under 13 to engage in sexual activity

☐   The Sexual Offences Act 2003 – Section 10. Causing or inciting a child to engage in sexual activity.

- The Sexual Offences Act 2003 – Section 12. Causing a child to watch a sexual act

- The Sexual Offences Act 2003 – Section 13. Child sex offences (section 10, 11 and 12) but committed by children (offender is under 18).

- The Serious Crime Act 2015 - Part 5. Protection of Children - Section 67. Sending a child sexualised communication.

More information about these offences can be found within the legal framework section of the policy template.

Schools and settings may wish to highlight responses to online child sexual abuse within existing school policies and procedures rather than within the online safety policy.

The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff, and parents/carers.

- North Oxfordshire Academy views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead (name and role).

- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Local Police.

- If the school are made aware of incident involving online child sexual abuse of a child, then the school will:
    o Act in accordance with the school's child protection and safeguarding policy and the relevant Local Safeguarding Child Boards procedures.
    o Immediately notify the designated safeguarding lead. o Store any devices involved securely.
    o Immediately inform local police via 101 (using 999 if a child is at immediate risk) or alternatively to CEOP by using the Click CEOP report form: http://www.ceop.police.uk/safety-centre/
    o Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse
    o Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    o Make a referral to children's social care (if needed/appropriate).
    o Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    o Inform parents/carers about the incident and how it is being managed.

-
-
  - o Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.
- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.

  The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.

- If pupils at other schools are believed to have been targeted, then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.

- The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button the school website homepage and on intranet systems.

Responding to concerns regarding Indecent Images of Children (IIOC)

Discussion:

Schools and settings must be aware of and understand the law regarding indecent images of children. Specifically, (but not limited to):

- The Sexual Offences Act 2003 (England and Wales) defines a child, for the purposes of indecent images, as anyone under the age of 18. The Civic Government (Scotland) Act, 1982 replicates this.
- The Sexual Offences Act 2003 (England and Wales) provides a defence for handling potentially criminal images and this is supported by a Memorandum of Understanding which provides guidance on what is and is not acceptable.

It is an offence to possess, distribute, show and make indecent images of children. Making of and distributing indecent images of children includes printing and viewing them on the internet otherwise known as 'downloading'. More information about these offences can be found within the legal framework section.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of school computer equipment, then schools should determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible if the offence is deemed to be out of the remit of the school to deal with. If schools are unsure if an issue is of a criminal nature, then the Designated Safeguarding Lead should seek advice from the Education Safeguards Team or Local Police.

Where it is determined that an offence has been committed and that a police investigation is warranted, all measures to preserve evidence should be undertaken. If an officer decides that equipment needs to be seized,

-

then they will need to determine if the equipment is networked. If in doubt as to whether the server should be seized or not, officers should seek advice from the Police Digital Forensic Unit, as seizure of the server will have a significant impact on the school. It is essential that schools are aware of this possibility, and they should ensure that measures are in place to enable the school's computer network to continue functioning should this situation arise.

In cases where a suspect picture or photograph is discovered it should also be borne in mind that a person could be guilty of the offence to 'Make' and 'Distribute' if they print or forward the image. There is a defence in law for police investigating crimes in these circumstances — in some cases, it may still be necessary for that person, or others (for example a person to whom an accidental find is reported), to knowingly "make" another copy of the

photograph or pseudo-photograph in order that it will be reported to the authorities, and clearly it is desirable that they should be able to do so without fear of prosecution. This does not mean that schools should forward, save or print indecent images of children and as soon as schools are made aware that an image may be illegal, appropriate advice must be sough immediately. Schools should be aware that all copies (including digital or printed copies) of indecent images of children will be seized.

In all cases, a detailed statement may be obtained to assist those who investigate the offence. The following information should be included in the statement:

- The identity of any material witnesses
- The name of the Internet service provider (ISP) or mobile telephone service provider in the case of images received through a telephone
- If known, the web address, name of the app or website through which the image was found or received;
- Any passwords or other procedure required to gain access to the website
- If known, the identity of the person who sent the image
- Any details relating to those involved e.g. email address or screen names
- The reason for any delay in reporting the incident to the police (to assist investigators).

In the case of offences involving mobile phones or devices ("sexting"), the likelihood is that issues will in the main be resolved by the school. Should an incident arise which is deemed to be of a serious nature and necessitates criminal investigation it may require the seizure of the phone/device. Schools and settings should ensure the existing policies regarding seizing and searching are robust and up-to-date.

Schools and settings may wish to highlight responding to concerns regarding Indecent Images of children within existing policies and procedures rather than within the online safety policy.

- The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
- The school will take action to prevent accidental access to Indecent Images of Children (IIOC); for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or local police.
- If the school/setting are made aware of Indecent Images of Children (IIOC) then the school will: o Act in accordance with the school's child protection and safeguarding policy and the relevant Local Safeguarding Child Boards procedures.
    - o Immediately notify the school Designated Safeguard Lead.
    - o Store any devices involved securely.
    - o Immediately inform appropriate organisations e.g., the Internet Watch Foundation (IWF), local police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, then the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
- If the school are made aware that indecent images of children have been found on the schools electronic devices then the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any/all copies that exist of the image, for example in emails, are deleted, following advice from the police.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
  - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
  - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
  - Follow the appropriate school policies regarding conduct.

Responding to concerns regarding radicalisation or extremism online

Discussion:

Schools and settings should be mindful of the specific responsibilities and requirements place upon them under the Prevent Duty https://www.gov.uk/government/publications/protecting-children-fromradicalisationtheprevent-duty

From 1st July 2015 specified authorities, including all schools are subject to a duty under section 26 of the Counter-Terrorism 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

statutory Prevent guidance summarises the requirements on schools as undertaking risk assessment, working in partnership, staff training and IT policies.

Schools are expected to assess the risk of children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology which includes a range of extremism views including the far right. Schools should have clear procedures in place for protecting children who are identified to be at risk of radicalisation. These procedures may be set out in existing safeguarding policies and it is not necessary for schools and colleges to have distinct policies on implementing the Prevent duty. The online safety policy will be an important part of this role as it will highlight the action that the school will take to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place which takes into account the needs of the schools community. Schools should ensure that online safety education highlights the risks of extremist content online, especially regarding the use and power of social media as a tool in radicalisation.

When ensuring appropriate filtering is in place, schools should be mindful to act in accordance with the law, much like when ensuring the filtering blocks other forms of illegal content. It should also be noted that radicalisation and extremist views can be shared and accessed on variety of platforms, including user generated or social media sites such as Facebook and YouTube and schools should make filtering decisions with this in mind. The way in which the monitoring of internet and network use is managed will be down to individual schools to decide and implement so as to meet their specific needs and requirements, for example taking into account the curriculum and also the needs and abilities of the community e.g. pupils or staff with EAL. The school (Head and Governing Body) needs to be able to satisfy itself that appropriate safeguarding measures (all reasonable precautions) are being taken to identify any activity which indicates that pupils or staff may be at risk of harm (or indeed putting others at risk). Leaders will need to ensure that appropriate time and resources are available to ensure that this is done sufficiently for a range of risks which will include radicalisation and extremism from a variety of perspectives as well as grooming and child sexual exploitation.

If schools/settings use devices which do not require pupils/staff to "login" to systems (such as iPads) to access the internet then they must ensure that there is appropriate mechanisms in place to log which member of the community has access to which devices to ensure that if concerns are identified, the school can trace users.

Staff with the responsibility for managing and monitoring the school filtering and network must have appropriate resources available to them as well as training and support to ensure that this can be carried out in both a manageable and a safe way. These decisions must be documented within the appropriate school policies (especially the school AUP) and be supported with training etc. and supervision all staff involved as well as the wider whole school staff and pupil group.

Schools should always be aware that simply relying on filtering to prevent radicalisation will not be sufficient as children are likely to have access to a range of devices within the home which may not be filtered or monitored, education around safe use if therefore essential. As all safeguarding risks, all members of staff should be alert to changes in children's behaviour which may indicate that they may be at risk or in need of specific help or protection. All members of staff should receive appropriate training to enable them to explore their responsibilities with regards to prevent for safeguarding pupils and adults within the school community.

School staff should also understand when it is appropriate to make a referral to the Channel programme using the Prevent Referral form. Channel is a programme which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. It provides a mechanism for schools to make referrals if they are concerned that an individual might be vulnerable to radicalisation. An individual's engagement with the programme is entirely voluntary at all stages.

Schools and settings may choose to highlight the overall response to the Prevent duty within existing policies and procedures rather than within the online safety policy.

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils. Schools will need to highlight specifically how internet use will be monitored either here or within subsequent sections.

- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school safeguarding policy.

Responding to concerns regarding cyberbullying

Discussion:

Online or cyberbullying can be defined as the use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone. Cyberbullying is becoming increasingly prevalent with the rapid advances and use of modern technology. Mobile, internet and wireless technologies have increased the pace of communication and brought significant benefits to users worldwide, but their popularity provides increasing opportunity for misuse through 'cyberbullying', with worrying consequences. It's crucial that children and young people as well as adults, use their devices and the internet safely and positively and they are aware of the consequences of misuse. As technology develops, bullying techniques can evolve to exploit it.

When children or adults are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if those around them do not understand online bullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

Cyberbullying may not always be intentional and repeated in the same way that traditional offline bullying is. Repeated harassment online could include an initial concern which is then shared or endorsed by others such as by "liking", "sharing" or "commenting". People may not feel that they are bullying by doing this and single issue may become more serious. It is very important that all incidents of online abuse are addressed as early as possible to prevent escalation

Education staff, parents and young people have to be constantly vigilant and work together to prevent this and tackle it wherever it appears. Cyberbullying is a method of bullying and should be viewed and treated the same as "real world" bullying and can happen to any member of the school community.

It is essential that young people, school staff and parents and carers understand how online can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

- every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents
- gives headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

Where online bullying which takes place outside school is reported then it must be investigated and acted on.

Under the Children Act 1989 a bullying incident should be addressed as a child protection concern when there is 'reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm' and Emotional abuse highlights the impact of online bullying. Where this is the case, the school staff should report their concerns to the Education Safeguards Team. Even where safeguarding is not considered to be an issue, schools may need to draw on a range of external services to support the pupil who is experiencing bullying, or to tackle any underlying issue which has contributed to a child doing the bullying.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications both on and offline could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed they should seek assistance from the police

Additional advice and information can be found at http://www.kelsi.org.uk/support-for-childrenandyoungpeople/child-protection-and-safeguarding/e-safety/cyberbullying.For more information please read
"Preventing and Tackling Bullying: Advice for School Leaders, Staff and Governing Bodies"
https://www.gov.uk/government/publications/preventing-and-tackling-bullying.

Childnet International have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: www.childnet.com.

- Cyberbullying, along with all other forms of bullying, of any member of North Oxfordshire Academy will not be tolerated.

- All incidents of online bullying reported will be recorded.

- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.

- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or local police.

United Learning
The best in everyone™
Ambition ▪ Confidence ▪ Creativity ▪ Respect ▪ Enthusiasm ▪ Determination

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.

- Sanctions for those involved in online or cyberbullying may include:
    - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools antibullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils involved in online bullying will be informed. o The Police will be contacted if a criminal offence is suspected.

Appendix B Notes on the Legal Framework

Many young people and indeed some staff and adults use the Internet regularly without being aware that some of the activities they take part in are potentially illegal.

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It is not professional advice and schools should always consult with their Area Safeguarding Adviser or the Education Safeguarding Adviser (Online Protection) from the Education Safeguarding Team, Legal representation, Local Authority Designated Officer or Kent Police if they are concerned that an offence may have been committed.

Please note that the law around this area is constantly updating due to the rapidly changing nature of the internet and this list is not exhaustive.

Data protection and Computer Misuse

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. 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.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the 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.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information

Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

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 someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

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

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the interception of communications and makes 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.

Obscene Content and Harassment

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence and this includes electronic transmission. For the purposes of the Act an article is deemed to be obscene if its effect is to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the content. This offence can result in imprisonment for up to 5 years.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message 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. This offence can result in imprisonment for up to 2 years.

Protection from Harassment Act 1997

This Act is relevant for incidents that have happened repeatedly (i.e. on more than two occasions). The Protection from Harassment Act 1997 makes it a criminal and civil offence to pursue a course of conduct which causes alarm and distress, which includes the publication of words, which he/she 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.

The victim can also bring a civil claim for damages and an injunction against the abuser, although in reality this is a remedy that is only used by individuals with the financial means to litigate, and only possible if the abuser can be identified, which is not always straightforward.

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.

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.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Racial and Religious Hatred Act 2006

This Act makes 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.

Libel and Privacy Law

These matters will be dealt with under civil rather than criminal law.

Libel is defined as 'defamation by written or printed words, pictures, or in any form other than by spoken words or gestures' and as such could the author could be held accountable under Defamation law which was created to protect individuals or organisations from unwarranted, mistaken or untruthful attacks on their reputation. Defamation is a civil "common law" tort in respect of which the Defamation Acts of 1952 and 1996 provide certain defences. It applies to any published material that damages the reputation of an individual or an organisation, and it includes material published on the internet.

A civil action for defamation can be brought by an individual or a company, but not by a public authority. Where defamatory material is posted on a website, the person affected can inform the host of its contents and ask the host to remove it. Once the host knows that the material is there and that it may be defamatory, it can no longer rely on the defence of innocent dissemination in the Defamation Act 1996. This means that the person affected could (if the material has been published in the jurisdiction, i.e. in England and Wales) obtain a court order (an injunction) to require removal of the material, and could sue either the host or the person who posted the material for defamation.

If social media is used to publish private and confidential information (for example breaches of data protection act) about an individual, then this could give rise to a potential privacy claim and it is possible for individuals to seek an injunction and damages.

Education Law

Education and Inspections Act 2006

Section 89 of the states that every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents. This act (89.5) gives headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

The Education Act 2011

Section 13 makes it an offence to publish the name of a teacher who is subject to an allegation until such a time as that they are charged with an offence. All members of the community need to be aware of the importance of not publishing named allegations against teachers online as this can lead to prosecution. Schools should contact the LADO team for advice.

Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. The DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies"
www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screeningsearchingandconfiscation

Sexual Offences

Criminal Justice and Courts Bill 2015

Section 33 makes it an offence to share private, sexual materials, either photos or videos, of another person without their consent and with the purpose of causing embarrassment or distress, often referred to as "revenge porn". The offence applies both online and offline and to images which are shared electronically or in a more traditional way so includes the uploading of images on the internet, sharing by text and e-mail, or showing someone a physical or electronic image. This offence can result in imprisonment for up to 2 years.

Sending images of this kind may, depending on the circumstances, also be an offence under the Communications Act 2003 or the Malicious Communications Act 1988. Repeated behaviour may be an offence under the Protection from Harassment Act 1997. This law and the term "revenge porn" only applies to images or videos of those over 18.

Sexual Offences Act 2003

There are many offences under the Sexual Offence Act 2003 which can be related to or involve the misuse of technology. This includes (but is not limited to) the following points.

Section 15 - Meeting a child following sexual grooming.

The offence of grooming is committed if someone over 18 has communicated with a child under 16, at least twice (including by phone or using the Internet) and meets them or travels to meet with them anywhere in the world with the intention of committing a sexual offence. This offence can result in imprisonment for up to 10 years.

Causing or inciting a child under 16 to watch or take part in a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification .

- **Section 8. Causing or inciting a child under 13 to engage in sexual activity** (Can result in imprisonment for up to 14 years)
- Section 9. Sexual Activity with a child (Can result in imprisonment for up to 14 years)
- **Section 10. Causing or inciting a child (13 to 16) to engage in sexual activity** (Can result in imprisonment for up to 14 years)
- **Section 11. Engaging in sexual activity in the presence of a child** (Can result in imprisonment for up to 14 years)
- **Section 12. Causing a child to watch a sexual act** (Can result in imprisonment for up to 10 years)
- **Section 13. Child sex offences committed by children** (offender is under 18) (Can result in imprisonment for up to 5 years)
- Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Section 16 - Abuse of position of trust: sexual activity with a child.

It is an offence for a person in a position of trust to engage in sexual activity with any person under 18 with whom they know as a result of being in their professional role. It is also an offence cause or incite a child with whom they are in a position of trust to engage in sexual activity, to engage in sexual activity in the presence of a child

with whom they are in a position of trust, or cause a child with whom they are in a position of trust to watch a sexual act. Typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust and this can result in imprisonment for up to 5 years.

Indecent Images of Children

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom under two pieces of legislation; **Criminal Justice Act 1988**, section 160 and **Protection of Children Act 1978**, section 1.1.a. Indecent images of children are images of children (under 18 years) depicting sexual posing, performing sexual acts on themselves or others, animals or sadomachisism.

A child for these purposes is considered to be anyone under the age of 18. An image of a child also covers pseudophotographs (digitally collated or otherwise). This offence can include images taken by and distributed by the child themselves (often referred to as "Sexting", see section 9.1). Viewing an indecent image of a child on your computer or phone means that you have made a digital image and printing/forwarding/sharing/publishing can be considered to be distribution. A person convicted of such an offence may face up to 10 years in prison.

Criminal Justice and Immigration Act 2008

Section 63 makes it an offence to possess "extreme pornographic images". 63 (6) identifies that such images must be considered to be "grossly offensive, disgusting or otherwise obscene". Section 63 (7) includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties for possession of extreme pornographic images can be up to 3 years imprisonment.

The Serious Crime Act 2015

Part 5 (Protection of Children) section 67 makes it a criminal offence for an adult (person aged over 18) to send a child (under 16) sexualised communications or sends communications intended to elicit a sexual communications. The offence is committed whether or not the child communicates with the adult. Penalties for sexual communication with a child can be up to 2 years imprisonment.

Section 69 makes it an offence to be in possession of paedophile manuals, information or guides (physically or electronically) which provide advice or guidance on sexually abusing children. Penalties for possession of such content can be up to 3 years imprisonment.

This law also removed references in existing legislation to terms such as child prostitution and child pornography and identified that this should be viewed to be child sexual exploitation.

Appendix C Online Safety (e-Safety) Contacts and Reference

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.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

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com
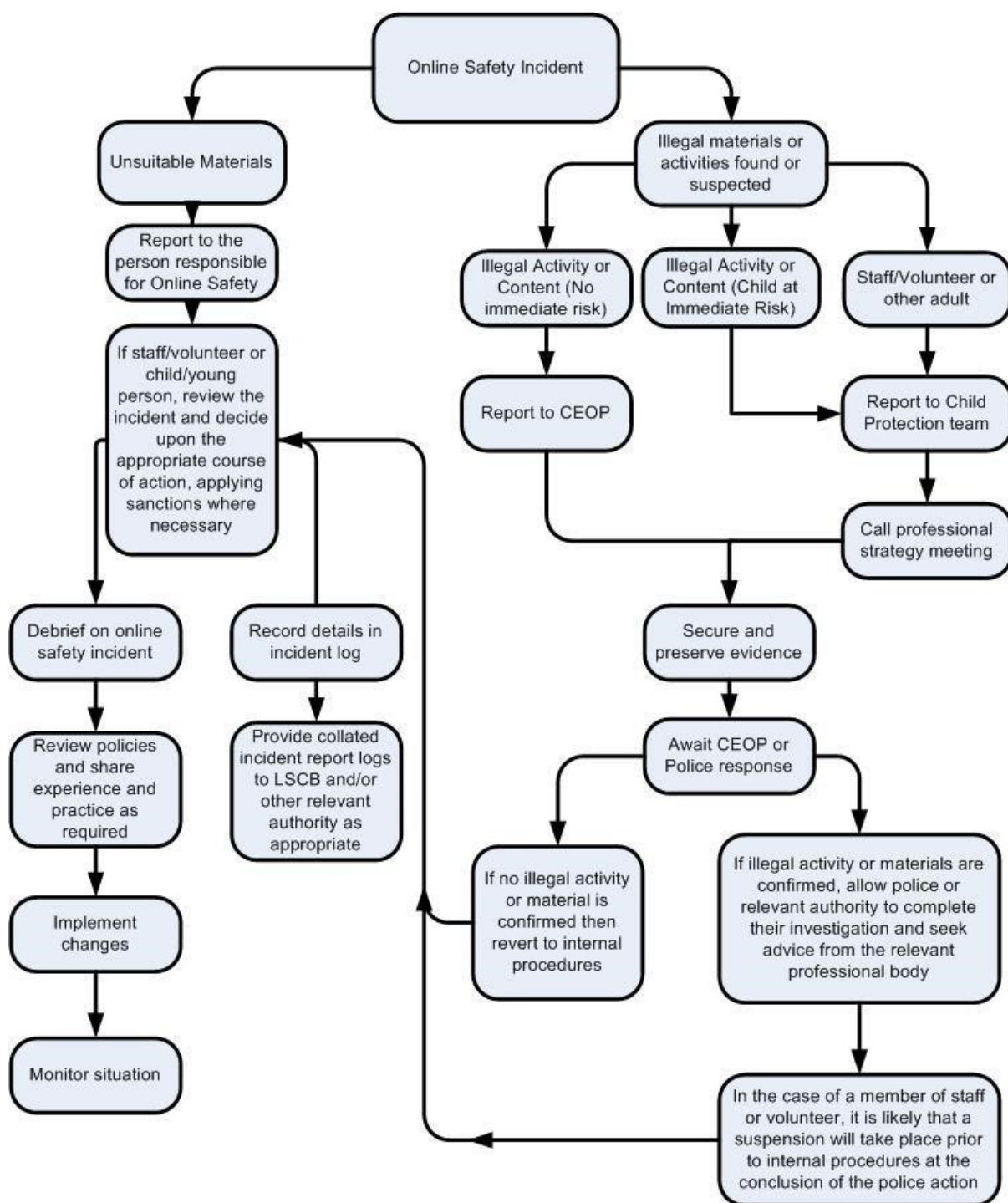
UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: https://360safe.org.uk/

Appendix D – Responding to Incidents of Misuse – Flowchart

Taken from the SWGFL - Responding to incidents of misuse – flow chart, part of their E-safety School Template Policies Document.

United Learning
The best in everyone™

Ambition   ■   Confidence   ■   Creativity   ■   Respect   ■   Enthusiasm   ■   Determination