ST IVES

HASLEMERE

St Ives School
HASLEMERE

ONLINE & E-SAFETY POLICY

Online and E-safety Policy

Contents

How to use this document

1. Creating an online safety ethos
    - 1.1. Aims and policy scope
    - 1.2. Writing and reviewing the online safety policy
    - 1.3. Key responsibilities of the community
        - 1.3.1. Key responsibilities of the management team
        - 1.3.2. Key responsibilities of the online safety/designated safeguarding lead
        - 1.3.3. Key responsibilities of staff
        - 1.3.4. Additional responsibilities of staff managing the technical environment
        - 1.3.5. Key responsibilities of children and young people
        - 1.3.6. Key responsibilities of parents/carers
2. Online communication and safer use of technology
    - 2.1. Managing the website
    - 2.2. Publishing images online
    - 2.3. Managing email
    - 2.4. Official video conferencing and webcam use
    - 2.5. Appropriate safe classroom uses of the internet and associated devices
    - 2.6. Management of school learning platforms/portals/gateways
    - 2.7. Appropriate and Safe use of AI
3. Policy decisions
    - 3.1. Recognising online risks
    - 3.2. Internet use within the community
    - 3.3. Authorising internet access
4. Engagement approaches
    - 4.1. Engagement of children and young people
    - 4.2. Engagement of children and young people who are considered to be vulnerable

4.3. Engagement of staff

4.4. Engagement of parents/carers

5. Responding to online incidents and concerns

6. Data Protection

Appendix A: (7) Procedures for responding to specific online incidents or concerns (including 'sexting', online child sexual abuse, indecent image of children, radicalisation and cyberbullying)

Appendix B: (8) Notes on the legal framework

Appendix C: (9) Online safety contacts and references

Appendix D: (10) Responding to Incidents of Misuse – Flowchart

Appendix E: (11) Online Safety Incident Record

Appendix F (12) Online Safety Incident Log

	DATE	NAME
AUTHORISED	January 2026	Kay Goldsworthy
POLICY REVIEWED	January 2026	Kay Goldsworthy
NEXT REVIEW DATE	January 2027	

1. Creating an Online Safety Ethos

*1.1 **Aims and policy scope***

- St Ives School 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, tablets, mobile phones or games consoles.
- St Ives School 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.
- St Ives School has a duty to provide the school community with Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the school's management functions. St Ives school also identifies that with this there is a clear duty to ensure that children are protected from potential harm online.
- The purpose of St Ives School's online safety policy is to:
    - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that St Ives School is a safe and secure environment.
    - Safeguard and protect all members of the St Ives School community online.
    - Raise awareness with all members of the St Ives 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, Anti-Bullying, Behaviour, Data Protection and Privacy Policies, Acceptable Use Policies, and relevant curriculum policies including Computing and Personal Social Health Education (PSHE) and the RSE policy.

*1.2 **Writing and reviewing the online safety policy***

- St Ives School 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 School has appointed a member of the Governing Body to take lead responsibility for online safety (e-Safety).
- 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) Lead is:
  - **Curriculum:** Nicola Smith
  - **Systems:** Charlie Baddock.

The School Designated Safeguarding Leads (DSL) are Kay Goldsworthy (School), Jade Vaus (DSL EYFS) and Nicola Smith (Deputy DSL).

The School Online Safety (e-Safety) lead for the Governing Body is Karen Laurie.

The date for the next policy review is January 2027

1.3 Key responsibilities of the community

1.3.1 Key responsibilities of the school/setting management team are:

- 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 appropriate 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.
- Ensuring 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 (e-Safety lead.

1.3.2 Key responsibilities of the Online Safety Lead (with support from the Designated Safeguarding Leads) 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 e.g. UK GDPR.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the school's safeguarding recording structures and mechanisms.
- 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.
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually).
- 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.

1.3.3 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 only 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.

1.3.4. 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 / 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 as soon as they become aware of them 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 information, as determined by Online 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.

1.3.5 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 technology and behaving safely and responsibly to limit those risks.

1.3.6. 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.
- 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 approved systems 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.

2. Online Communication and Safer Use of Technology

2.1 Managing the school/setting website and social media accounts.

- The school will ensure that information posted on the school website meets requirements e.g. for ISI.
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal contact details 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.
- Pupils' work will only be published with parents/carers permission.
- The administration and monitoring of school social-media accounts is overseen by the Headteacher and Marketing Manager.
- As part of social-media engagement, the school will proactively monitor internet public postings about the school.

2.2 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 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.

2.3 Managing email

- Children do not use email as an everyday form of communication. When email is used e.g. as part of a staff led curriculum task, it is for St Ives internal access only.
- All members of staff and governors 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.
- Access in school to external personal email accounts may be blocked.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- 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 Office 365 in accordance with UL data sharing policy / data protection legislation. (UK GDPR)
- Caution should be taken on opening emails with attachments or clicking on links within; being conscious of the risks from malware.
- Messages sent to external organisations should be written carefully, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4 Official video conferencing 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 when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.
- Staff will ensure that external videoconferences 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 in school.
- Videoconferencing will be supervised appropriately for the pupils' age and ability. It will only be carried out under teacher supervision within the context of a teacher led lesson, assembly or after school club.
- 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/parents. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start. 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.

2.5 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.
- 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.

- 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 will be appropriate to their age and ability.
    - At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with some directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
    - At Key Stage 2 pupils will be supervised. Online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
- All school owned devices will be used in accordance with the School Acceptable Use Policy and with appropriate safety and security measures in place. Apps are not to be downloaded without permission of the SMT. No linked bank account is evident on mobile technologies, thus avoiding in app purchases being made.
- 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 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.

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

Currently the school does not have a Learning Platform, but this policy will be revised considering any changes in this regard.

2.7 Appropriate and safe use of AI.

- The use of Artificial Intelligence (AI) has potential to enhance teaching and learning at St Ives School when used responsibly.
- All use of AI must be ethical; respecting privacy, promoting fairness and preventing discrimination.
- Its use should safeguard staff and student data in accordance with UK GDPR.
- It should be evaluated critically, with an awareness of potential inaccuracy and bias in its content, as well as of its assets and limitations. Its use at St Ives School should seek to combine recognition of AI's educational benefits with an understanding that it is not a replacement for the creativity, intuition and understanding of a human being.
- Use of AI should encourage active engagement, independent learning and thinking rather than stifle such skills and attributes integral to teaching/ learning. Users should be mindful of the potential of AI to impact both positively and negatively on mental health.
- Appropriate use of AI incorporates the responsibilities, safe practices and safeguarding procedures of this policy.

3. Policy Decisions

3.1. Reducing online risks

- St Ives School 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/ Data Protection Impact 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. The filtering system is Securly.
- 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.

3.2. Internet use throughout the wider school/setting community

- The school will liaise with United Learning and local bodies 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. There is a designated guest WIFI.

3.3 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).

4. Engagement Approaches

4.1 Engagement and education of children and young people

- An online safety (e-Safety) curriculum will be taught throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils. The curriculum will cover the main areas of risk - Content, Contact, Conduct and Commerce.
- Education about safe and responsible use will precede internet access.
- Pupils 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 across the Key Stages.
- The pupil Acceptable Use expectations and Posters will be posted in 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 pupils' needs.

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

- St Ives School 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).

4.3 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 highlight 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.

4.4 Engagement and education of parents and carers

- St Ives School recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations e.g. in newsletters, letters, the school prospectus and on the school website.
- 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 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.

5. 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 Surrey Safeguarding 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 protocols around 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 Safeguarding 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 Authority Safeguarding Team to communicate to other schools/settings in the area.
- Parents and children will need to work in partnership with the school to resolve issues.

6. Data Protection and Back Ups.

- Staff should report all incidents where data protection may have been compromised to the Data Protection Officer. In the event of a data breach, a log will be kept. If this is likely to result in risk to individuals, ICO will be notified within 72 hours of becoming aware. Where there is high risk to individuals, the individual (data subject) will be informed without delay. All online activities at St Ives school whether internal or/and using third parties will be checked for UK GDPR compliancy. All St Ives staff are DBS checked and records are held in secure central systems. We transfer personal data safely where needed e.g. Data to government via secure access and personal data internally via SharePoint/ One Drive link/Isams/ CPoms. Backups are undertaken and stored in the cloud (SharePoint). Staff have secure access on the network to store sensitive information, documents or photographs. We comply with the WEEE directive on equipment disposal and UL policy/use of an approved supplier.

Appendices

Appendix A (7)

Procedures for Responding to Specific Online Incidents or Concerns

7.1 Responding to concerns regarding Self-Generated Indecent Images.

St Ives School ensures that all members of the community are made aware of the social, psychological and criminal consequences of sharing, possessing and creating incident images of children (known as "sexting").

- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- St Ives School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by a Designated Safeguarding Lead.
- If the school are made aware of an incident involving indecent images of a child, the school will:
  - Act in accordance with the school's safeguarding policy and the relevant Local Safeguarding Team procedures.
  - 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/the police. 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 an exceptional, clear need or reason for the DSL (or equivalent) 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 take action 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 as set out in Sharing nudes and semi-nudes: how to respond to an incident (24) and Sharing Nudes and semi-nudes: Advice for education settings working with children and young people. (2020 –updated 24)
- The school will ensure that all members of the community are aware of sources of support.

7.2. Responding to concerns regarding Online Child Sexual Abuse

- St Ives School will ensure that staff are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns. Children will be warned in age-appropriate ways such as

through encouraging them to talk to a responsible adult if upset by anything online, to keep personal information safe and not to talk to strangers online.

- 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.
- St Ives School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by a Designated Safeguarding Lead.
- 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 an incident involving online child sexual abuse of a child, then the school will:
    - Act in accordance with the school's child protection and safeguarding policy and the relevant Local Safeguarding procedures.
    - Immediately notify the designated safeguarding lead.
    - Store any devices involved securely.
    - Immediately inform local police via 101 (using 999 if a child is at immediate risk) or alternatively CEOP by using the Click CEOP report form: http://www.ceop.police.uk/safety-centre/
    - Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to Local Authority Safeguarding team (if needed/appropriate).
    - 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.
    - Inform parents/carers about the incident and how it is being managed.
    - 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 act 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 Local Authority 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 on the school website.

7.3 Responding to concerns regarding Indecent Images of Children (IIOC)

- St Ives School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The school will take action regarding 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) e.g. 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:

    - Act in accordance with the school's child protection and safeguarding policy and the relevant Local Authority Safeguarding procedures.
    - Immediately notify the school Designated Safeguard Lead.
    - Store any devices involved securely.
    - 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 school's 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 Headteacher/ Designated Safeguarding Lead is informed 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.

7.4. Responding to concerns regarding radicalisation or extremism online

- 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. .
- 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 and Prevent.

7.5 Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of St Ives School community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- 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.
- 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 anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils involved in online bullying will be informed.
    - The Police will be contacted if a criminal offence is suspected.

Appendix B (8)

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education and Working together to safeguard children. It also refers to the DfE's guidance on : the Prevent Duty

The following also relate to it:

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.

UK GDPR (General Data Protection Regulation)

The UK GDPR states

a) Personal data must be processed according to the 6 data protection principles:

- Processed lawfully, fairly and transparently.
- Collected only for specific legitimate purposes.
- Adequate relevant and limited to what is necessary.
- Accurate and up to date.
- Stored only for as long as necessary.
- Ensure appropriate security, integrity and confidentiality.

b) Accountability and governance

(Structure roles/responsibilities, record of data processing activities, data protection policy, data protection impact assessments for high risk processing, security, training and Data Protection Officer appointed)

c) Data Protection by design and by default. (Data protection practices and safeguards from beginning of processing)

d) Valid consent-There are stricter rules for consent. Silence, pre-ticks and inactivity will no longer suffice as consent. Consent can be withdrawn.

e) Privacy Rights of Individuals-Rights have been enhanced. An individual has (with some exceptions):

- The right to access personal data:
- The right to be informed of how their data is being used.
- The right to have incorrect data updated.
- The right (with exceptions) to have personal data erased.
- The right to stop/ restrict the processing of their data.
- The right to object.
- The right to move personal data.

Data Use and Access Act 2025

Updates on UK GDPR -Time limes for SARS modified where need to clarify information requester seeking and update on overly broad SAR requests. Update on facilitating the DP complaints process, Information on AI and development of a robust , thoughtful, measured approach towards it.

The Computer Misuse Act 1990 (sections 1 - 3) (Review published Feb 23)

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 (Reissued July 23) Investigatory Powers Act 2016

The Regulation of Investigatory Powers Act 2000 (RIPA) and Investigatory Powers Act 2016 regulate the interception of communications and make 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.

Online Safety Act 2023 (published 24- latest update 25)

A set of laws that protects children and adults online. It puts a range of new duties on social media companies and search services making them more responsible for their users' safety on these platforms.

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.

Employment Right Act 2025 (ERA 2025)

Gives employers a proactive duty to prevent sexual harassment and protect staff from third party harassment.

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.

Counter Terrorism and Border Security Act 2019

Amends some terrorism offences to update them to digital age, patterns of radicalisation and developments in terrorist threats. Allows Secretary of State to designate an area outside of UK which is associated with terrorism where offence to UK national to enter or remain in without reasonable excuse or exempt purpose and amends police powers to manage risk and investigate terrorism offences.

Counter Terrorism and Security Act 2015

Prevent Duty- (2015 –Last revision March 24) is the duty on specified authorities, including schools, in the exercise of their functions to have due regard to the need to prevent people being drawn into terrorism.

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/screening-searching-andconfiscation

Sexual Offences

Criminal Justice and Courts Act 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 pseudo-photographs (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 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 (9)

Online Safety (e-Safety) Contacts and Reference

National Links and Resources

Report Fraud https://www.reportfraud.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

NSPCC: www.nspcc.org.uk/onlinesafety

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

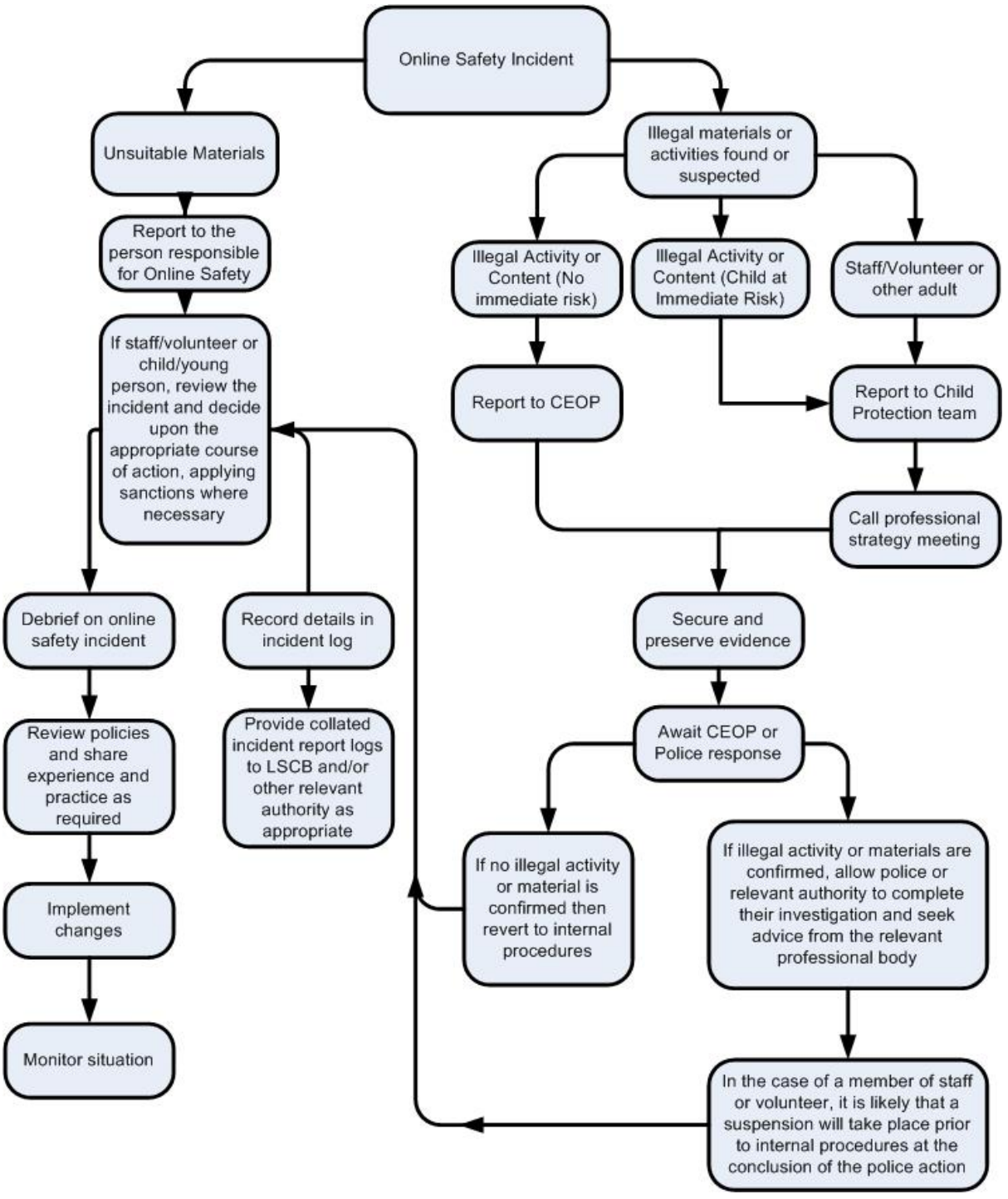
The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

CEOP Education: CEOP Education

UK Safer Internet Centre: www.saferinternet.org.uk

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

Appendix D (10) – 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.

Appendix E (11) -Online Safety Incident Record

Name of person reporting incident:				
Date of report:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young person	
Staff member(s)	
Parent(s)/ Carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)

Full description of the incident	What, when, where, how?
Name all if social media involved	
Evidence of the incident	Specify any evidence provided but do not attach

Immediate action taken following the reported incident:	
Incident reported to online safety Coordinator/DSL/ DSP/Headteacher	
Safeguarding advice sought, please specify	
Referral made to HCC Safeguarding	
Incident reported to police and/or CEOP	
Online safety policy to be reviewed/amended	
Parent(s)/carer(s) informed please specify	
Incident reported to social networking site	
Other actions e.g. warnings, sanctions, debrief and support	
Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery	

Brief summary of incident, investigation and outcome (for monitoring purposes)	

Appendix F (12)-Online Safety Incident Log

Summary details of ALL online safety incidents will be recorded on this form by the online safety coordinator or other designated member of staff. This incident log will be monitored and shared with SLT and, where required, Governors.

Date & time	Name of pupil or staff member Indicate target (T) or offender (O)	Nature of incident(s)	Details of incident (including evidence)	Outcome including action taken