

Introduction

This Staying Safe Online policy was approved by the <i>School Senior Leadership Team</i> :	September 2023
The implementation of this Staying Safe Online safety policy will be monitored by the:	<i>Online Safety Co-ordinator, Senior Leadership Team, OFG IT Department</i>
Should serious Online safety incidents take place, the following external persons / agencies should be informed:	<i>OFG IT Department, LA Safeguarding Officer. LADO, Police, National Quality & Audit Officer (Safeguarding)</i>

This policy should be read in conjunction with the OFG group **Staying Safe Online** policy:

Purpose

Heath Farm School and the Outcomes First Group places the safety of the children and adults we support as its highest priority. The purpose of this document is to set out the Group's policy for online safety and provide guidance to help keep the people we educate and care for safe online and when using digital devices.

Legal Framework & Government Guidance

Across the UK, criminal and civil legislation aims to prevent a range of abusive activities online including: stalking, harassment, improper use of any public communications, sending indecent, offensive, false or threatening communications and sending private sexual photos or videos of another person without their consent.

In March 2022, the UK Government introduced the Online Safety Bill to regulate providers of services which host online content generated by users, services which facilitate online interaction between users and search engines. This is a welcome step forward to help keep everyone safer online, however, the NSPCC has highlighted that it needs to go further to better tackle grooming and child abuse. As carers and educators of children and vulnerable adults, we must maintain our vigilance in helping those we support to stay safe online. For further information about the legal framework, please see: Key legislation for online abuse.

The Online Safety Bill is to have its third reading in the House of Lords on the 6th September 2023.

Group Policy

Governments of each UK nation have developed guidance to help keep children safe from online harm and abuse:

Advice to parents and carers on keeping children safe from abuse and harm - UK Government
 Online Safety Action Plan for Children and Young People in Wales - Welsh Government
 Safeguarding Children from Online Abuse - a guide for practitioners working with children in Wales has been produced by the Welsh Safeguarding Boards as part of the Wales Safeguarding Procedures.
 Internet Safety for children and young people: National Action Plan – Scottish Government

Scope

This policy applies to all services and settings within the Outcomes First Group operating in England, Wales and Scotland. It is applicable to residential care, schools, colleges and any further services the Group provides.

This policy and guidance document should be read in conjunction with the service's:

- Safeguarding Policy
- Anti-Bullying Policy and Guidance
- Gaming Devices Policy and Procedure
- Child Exploitation Policy and Guidance
- Protecting Children against Radicalisation Policy
- Use of Images & Audio Recording Policy (Clinical)
- Child-on-child abuse Policy/ Peer-on-peer abuse Policy

OFG Group Policy Statement

The Outcomes First Group is committed to keeping the children, young people and adults we support, educate and care for safe, whilst enabling them to enjoy their lives and have the same opportunities to explore the world as others.

Technology is part of everyday life for children and adults; it directly or indirectly affects almost every aspect of life. This provides many possibilities, including tools for learning, socialising, playing and helping young people find their place in the world. However, it also carries significant risks to which those we support can be more susceptible than their peers. Those already at risk offline are more likely to be at risk online.

Raising awareness of the potential risks and helping them to understand what they can do to keep themselves safe is essential for their well-being. Having regular conversations, understanding what they are using the internet for and assuring them there is a trusted adult they can talk to if anything upsets them online, will help to keep them safe.

Those working with children, young people and adults at risk are expected to support them to develop the skills they need to use the internet and social media safely for learning and enjoyment. Staff must keep children, young people and adults in their care as safe in the online world as in the real world.

For those we support who are non-verbal or have limited receptive and expressive communication and learning disabilities, more direct on-going observation of their technological use to support them is required to keep them safe, along with the direct modelling of safe online behaviour by those responsible for their care and education.

Online safety is important in all the Group's settings and services. Different services, and employees within them, may have different roles in keeping children, young people and adults safe online but it must always be treated as a high priority.

Schools and colleges

Digital technology, the internet and related applications provide a wealth of fabulous learning opportunities and have many positive uses in schools and colleges. Their use must be balanced with educating pupils about the risks and helping them to take a responsible and safe approach. Schools and colleges must help and support its children and young people to recognise and avoid online safety risks and to develop their digital resilience.

Pupils and students that have limited receptive and expressive communication and learning disabilities, will require more direct on- going observation of their technological use to support them is required to keep them safe.

Childnet provides a range of resources to support online safety for teachers: Help, advice and resources DFE has published Guidance for schools and colleges on Harmful online challenges and online hoaxes Guidance, which this includes advice on preparing for any online challenges and hoaxes, sharing information with parents and carers and where to get help and support.

Online safety should be covered in detail as part of the PSHE (Personal, Social, Health & Economic)/ PSE (Personal and Social Education) curriculum in schools.

The Group also requires safe and secure systems to be in place. An up-to-date Web Filtering Policy template is sent to each school annually and each school has a Mobile and Smart Technology Policy.

An annual review of the school's approach to online safety will take place, supported by an annual risk assessment that considers and reflects the risks children face. A free online safety self-review tool for schools can be found at <https://360safe.org.uk/>

Schools and colleges are encouraged to use the regular communications they have with parents and carers to reinforce the importance of children being safe online and keep them informed about what systems schools and colleges use to filter and monitor online use, what their children are being asked to do online at school or college, including the sites they will be asked to access, and be clear who from the school or college (if anyone) their child is going to be interacting with online.

The purpose of Heath Farm School (HFS) Staying Safe Online policy is to follow the guidance above, and to identify specific support and interventions that complement the working environments and set procedures of the school provision:

- Safeguard and protect all members of HFS community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

Scope of the HFS Policy

HFS believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and staff are protected from potential harm online.

- HFS identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- HFS believes that students should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all HFS staff including the governing body, teachers, support staff, 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 students and parents/carers
- This policy applies to all access to the internet and use of technology, including personal devices, or where students, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets, or mobile phones.

Heath Farm School will deal with such incidents within this policy in association with the behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The school has appointed Mark Jones as Designated Safeguarding Lead to be the online safety lead. HFS recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

HFS is part of OFG group who are responsible for the approval of the Staying Safe Online Policy and for reviewing the effectiveness of the policy. This will be carried out by the school's Headteacher reports and OFG receiving regular information about online safety incidents and monitoring reports on a termly basis.

Headteacher and Senior Leaders:

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the online Safety Co-ordinator.

The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

The Headteacher / Senior Leaders are responsible for ensuring that the online Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

Online Safety Co-ordinator:

HFS online safety co-ordinator is Mark Jones, Deputy Headteacher. His role as online safety co-ordinator will be to:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff.
- liaises with the Local Authority / relevant body.
- liaises with OFG ICT central staff.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression.
- receives reports of online safety incidents and creates a log of incidents via Sleuth to inform future online safety developments.
- discuss current issues, review incident logs with teachers and SLT.

ICT Services:

HFS will ensure:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority / other relevant body online Safety Policy / Guidance that may apply.

- that users may only access the networks and devices through a properly enforced password protection process.
- OFG web filtering policy is applied and updated on a regular basis.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and the online Safety Co-ordinator for investigation.
- that monitoring software / systems are implemented and updated as agreed by OFG and the school.
- In line with Keeping Children Safe in Education 2022, internet use is monitored and reviewed. Reports setting out all internet use will be sent by the OFG Group IT Department to Designated Safeguarding Leads every six months. This information will be stored by the school for a period of six months unless there are safeguarding concerns. If there are safeguarding concerns the information will be stored in line with statutory requirements for record retention.

Teaching and Support Staff

Are all responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices.
- they have read, understood the OFG ICT Acceptable Usage Policy and HFS CoC.
- they report any suspected misuse or problem to the Headteacher or online Safety Co-ordinator.
- all digital communications with students / students / parents / carers should be on a professional level and only carried out using official school systems/ ICT equipment.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- students / students understand and follow the online safety and acceptable use policies.
- students / students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned students / students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated safeguarding Lead (DSL)

Should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate online contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure all members of staff receive regular, up-to-date, and appropriate online safety training.
- Work with staff to co-ordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.

- Ensure that online safety is promoted to parents, carers, and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.

The combine role of Child Protection / Designated Safeguarding Lead and online Safety Officer is held by Mark Jones, Deputy Headteacher.

Education and engagement with students

- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst students by:
 - Ensuring education regarding safe and responsible use precedes internet access.
 - Including online safety in the PSHE, RSE and Computing programmes of study, covering use both at home school and home. Reinforcing online safety messages whenever technology or the internet is in use.
 - Educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval, and evaluation.
 - Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school will support students to read and understand the AUP in a way which suits their age and ability by:
 - Displaying acceptable use posters in all rooms with internet access.
 - Informing students that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
 - Rewarding positive use of technology by students.
 - Implementing appropriate peer education approaches through school council representatives.
 - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
 - Seeking student voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
 - Using support, such as external visitors, where appropriate, to complement and support the school's internal online safety education approaches.
 - are responsible for using the school's digital technology systems in accordance with the ICT Acceptable Use Policy.
 - have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
 - need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
 - will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
 - should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the schools online Safety Policy covers their actions out of school, if related to their membership of the school.

Vulnerable students

- HFS is aware that some students are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

HFS will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. HFS will take every opportunity to help parents understand these issues through newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support HFS in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- their children's personal devices in the school (where this is allowed)

Parents/carers will be given opportunities to attend a parent/carer workshop on online safety and receive weekly online safety safeguarding bulletin's to help raise their awareness in topical areas of concern. All parent and carers have access to the National Online Safety portal (NOS) and have individual login's.

<https://nationalonlinesafety.com/>

Policy Statements

Education - students / students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / students to take a responsible approach. The education of students / students in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety/online (PSHE/RSE integrated) curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Students / students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students / students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education - parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site online safety bulletins and workshops
- High profile events / campaigns e.g., **Safer Internet Day and school council initiatives.**
- Reference to the relevant online safety focussed web sites / publications

Education & Training - Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive online, e-safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
- The online Safety Co-ordinator (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / email bulletins and INSET days.
- The online safety Co-ordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Technical - infrastructure / equipment, filtering, and monitoring

OFG will be responsible for ensuring that all schools within their organisation infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

- Heath Farm School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school academy technical systems.
- Servers, wireless systems, and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users are responsible for the security of their username and password.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or another person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- Internet access is filtered for all users.
- The school has provided enhanced / differentiated user-level filtering.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / student's instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students / students will be selected carefully ensuring that Heath Farm School has written permission from the parent/Local Authority SW that the student's photo can be used for external publication.
- Students' / Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents/LACSW will be obtained before photographs of students / students are published on the school.
- Student's / Student's work can only be published with the permission of the student / student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant, and not excessive
- Accurate
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure
- Only transferred to others with adequate protection.
- In line with GDPR compliance and guidance.

Please refer to Heath Farm School Data Protection Policy for further guidance.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students / students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g., by remote access).
- Users must immediately report, to the e-safety coordinator, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / students or parents / carers (email, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while students / students at KS2 and above will be provided with individual school / academy email addresses for educational use.
- Students / students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for students and staff.

HFS provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Training to include acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures, and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

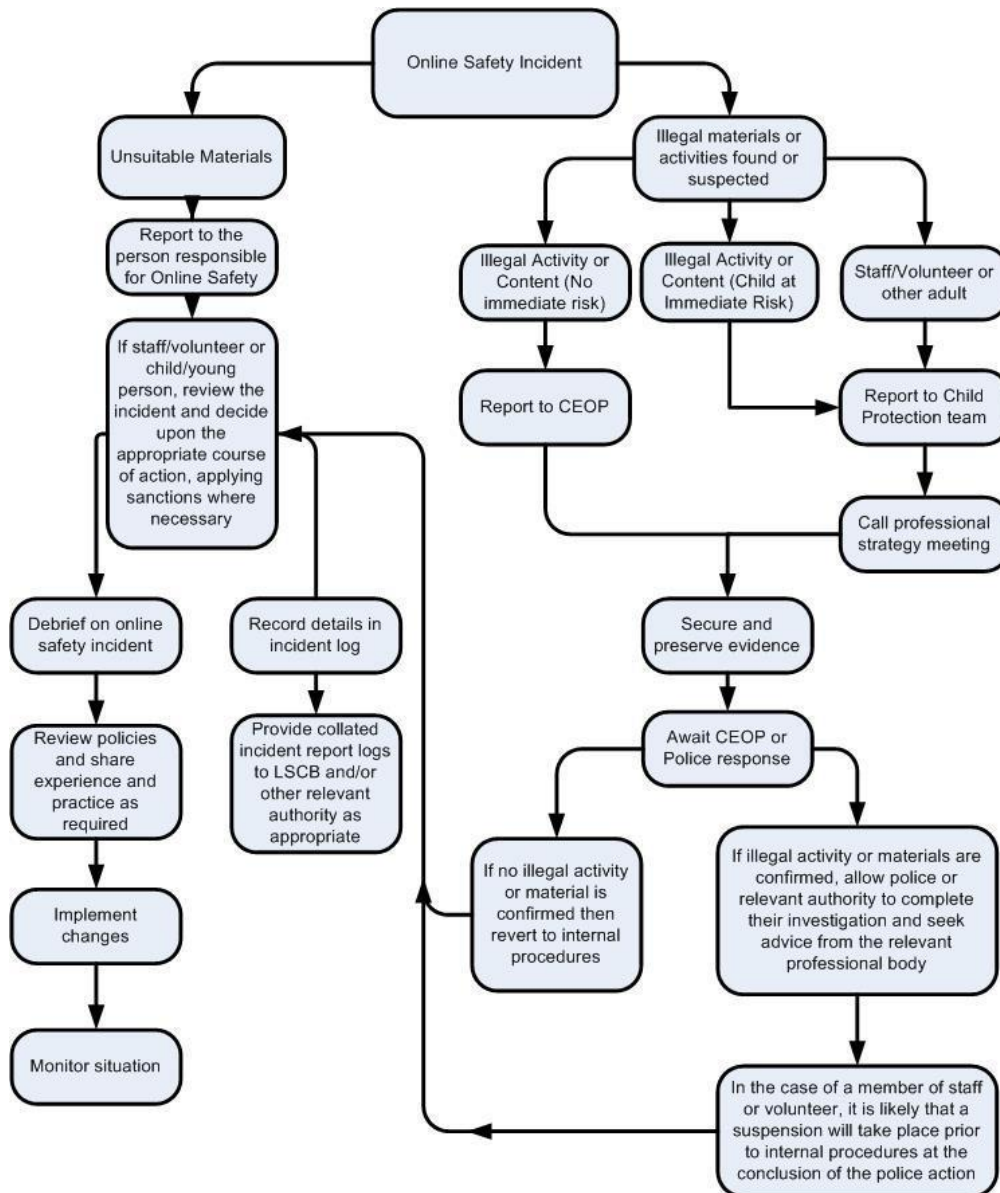
- No reference should be made in social media to students / students, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority or national / local organisation (as relevant).
 - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
 - incidents of ‘grooming’ behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - other criminal conduct, activity, or materials
 - **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Logical Consequences

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through Heath Farm School behaviour / disciplinary procedures.

Social Media

Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of HFS community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chat rooms and instant messenger.
- All members of HFS community are expected to engage in social media in a positive, safe and responsible manner, at all times.
- All members of HFS community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control student and staff access to social media whilst using school provided devices and systems on site.
- The use of social media during school hours for personal use is not permitted.
- Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of HFS community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour (PBRs) and Child protection (safeguarding) policies.

Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of conduct within the AUP.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may 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.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
 - Setting the privacy levels of their personal sites as strictly as they can.
 - Being aware of location sharing services.
 - Opting out of public listings on social networking sites.
 - Logging out of accounts after use.
 - Keeping passwords safe and confidential.
 - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of HFS on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework.

- Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with students and parents and carers

- All members of staff are advised not to communicate with or add as ‘friends’ any current or past students or current or past students’ family members via any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Headteacher.
- If ongoing contact with students is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to make contact with students or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from students and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

Students’ Personal Use of Social Media

- Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding students’ use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Students will be advised:
 - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name.
 - address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
 - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
 - Not to meet any online friends without a parent/carer or other responsible adult’s permission and only when a trusted adult is present.
 - To use safe passwords.
 - To use social media sites which are appropriate for their age and abilities.
 - How to block and report unwanted communications and report concerns both within school and externally.

Use of Personal Devices and Mobile Phones, plus Smart Watches

- HFS recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but technologies need to be used safely and appropriately within school.

Expectations

- All use of personal devices and mobile phones / smart watches will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-bullying, Behaviour, Child protection and Safeguarding. Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
- All members of HFS community are advised to take steps to protect their mobile phones or devices from loss, theft, or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
- All members of HFS community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy.
- All members of HFS community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school Behaviour or Child protection policies.

Staff Use of Personal Devices and Mobile Phones / Smart Watches

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Child protection, Data security and Acceptable use. Staff will be advised to:
 - Keep mobile phones and personal devices in a safe and secure place during lesson time e.g. locked in a locker/drawer.
 - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
 - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
 - Not to use personal devices during teaching periods, unless written permission has been given by the Headteacher, such as in emergency circumstances.
 - Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
 - Members of staff are not permitted to use their own personal phones or devices for contacting students or parents and carers.
 - Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead and/or Headteacher.
 - Staff will not use personal devices, such as: mobile phones, tablets or cameras:
 - To take photos or videos of students and will only use work-provided equipment for this purpose.
 - Directly with students and will only use work-provided equipment during lessons/educational activities.
 - If a member of staff breaches the school policy, action will be taken in line with the school behaviour and allegations policy.
 - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

Students' Use of Personal Devices and Mobile Phones / Smart Watches

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- **Student mobile phones and personal devices are not permitted to be used in specific areas within the school site and will be handed in to the class teacher/Tutor by 9.30 am each day and handed back to them at the end of day tutorial. If permitted by the class teacher /tutor the student mobile phones will only be accessed at break times. Failure to adhere to this expectation and breaches of the school policy will result in the parent/carer being called and either collecting the phone or the student's day will be ended.**
- **Students are not permitted to bring in Smart Watches due to the complexity of privacy setting and parental responsibilities.**
 - **The class teacher will use their discretion with Key Stage 4 students and Key Stage 5 students will be given the responsibility to have access to their personal devices, but they must follow the staff expectations of using their own personal devices.**
 - If a student needs to contact his/her parents or carers they will be allowed to use a school phone.
 - Parents are advised to contact their child via the school office during school hours; exceptions may be permitted on a case-by-case basis, as approved by the Headteacher. *E.g., if phones are allowed during break times.*
 - Mobile phones and personal devices must not be taken into examinations.
 - Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
 - School staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Bullying policy, or could contain youth produced sexual imagery (sexting).
 - Searches of mobile phone or personal devices will only be carried out in accordance with the school's policy.
 - If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Visitors' Use of Personal Devices and Mobile Phones / Smart Watches

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable use policy and other associated policies, such as: Anti-bullying, Behaviour, Child protection and Image use.
- The school will ensure appropriate signage and information is displayed/ provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.

Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
- Students, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.

- The school requires staff, parents, carers and students to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Kent Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

Concerns about Students Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSL will record these issues in line with the school's child protection policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher, according to the Allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Behaviour policy and Code of conduct.

Procedures for Responding to Specific Online Incidents or Concerns

Youth Produced Sexual Imagery or "Sexting"

- HFS recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will follow the advice as set out in the non-statutory UKCCIS guidance and KSCB guidance: "Responding to youth produced sexual imagery".
- HFS will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Dealing with 'Sexting'

Sexting can happen through sexually explicit text messages, provocative audio clips, suggestive selfies, or videos. No matter what form sexting takes, it should always be a consensual practice between two or more parties.

- If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:
 - Act in accordance with our Child protection and Safeguarding policies and the relevant

- Kent Safeguarding Child Board's procedures.
- Immediately notify the Designated Safeguarding Lead.
- Store the device securely.
- If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of student(s) involved, including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed. Make a referral to Specialist Children's Services and/or the Police, as appropriate.
- Provide the necessary safeguards and support for students, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with the school's Behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS guidance.
- Images will only be deleted once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.
- The school will act regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- The school will not:
 - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so. In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.
 - Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request students to do so.

Online Child Sexual Abuse and Exploitation

- HFS will ensure that all members of the community are aware of online child sexual abuse, including exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- HFS recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for students, staff, and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.
- The school will ensure that the 'Click CEOP' report button is visible and available to students and other members of the school community.

Dealing with Online Child Sexual Abuse and Exploitation

- If the school are made aware of incident involving online sexual abuse of a child, the school will:
 - Act in accordance with the school's Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
 - Immediately notify the Designated Safeguarding Lead.
 - Store any devices involved securely.
 - Immediately inform Kent police via 101 (or 999 if a child is at immediate risk)
 - Inform parents/carers about the incident and how it is being managed.

- Make a referral to Specialist Children’s Services (if required/ appropriate).
 - Provide the necessary safeguards and support for students, such as, offering counselling or pastoral support.
 - Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.
- The school will act regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
 - Where possible students will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report system available online.
 - If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
 - If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the Designated Safeguarding Lead.
 - If students at other schools are believed to have been targeted, the school will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at HFS Full details of how the school will respond to cyberbullying are set out in the Anti-bullying policy.

Online Hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at HFS and will be responded to in line with existing school policies, including Anti-bullying and Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Kent Police.

Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school. If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately, and action will be taken in line with the Child protection policy.
- If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the Child protection and Allegations policies.

Useful Links for Educational Settings

Kent Support and Guidance

Kent County Council Education Safeguarding Team:

- Education Safeguarding Adviser (Online Protection)

- E-Safety Development Officer
esafetyofficer@kent.gov.uk Tel: 03000 415797

Guidance for Educational Settings:

- www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
- www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
- www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
- Kent e-Safety Blog: www.kentesafety.wordpress.com

KSCB:

- www.kscb.org.uk

Kent Police:

- www.kent.police.uk or www.kent.police.uk/internetsafety
- In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Other:

- Kent Public Service Network (KPSN): www.kpsn.net
- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: www.eiskent.co.uk

National Links and Resources

- Action Fraud: www.actionfraud.police.uk
- CEOP:
 - www.thinkunow.co.uk
 - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
 - ChildLine: www.childline.org.uk
 - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
 - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

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

Helpful Resources

In addition to the websites mentioned in this document, the following links also provide helpful information:

NSPCC Keeping Children Safe Online Safety

NSPCC Online Safety Families Children with SEND Social Media Guidance for parents and carers

Cerebra - Learning Disabilities, Autism and Internet Safety

UKCIS (UK Council for Internet Safety)

Star SEND toolkit

Ambitious about Autism - Online safety information Stop It Now! (UK and Ireland)

Child Protection Scotland - Online Abuse