Online Safety Policy

Date Approved	**23rd November 2020**
Date of Next Review	**November 2022**
Policy Owner	**Computing Lead**
Approved by	**School Improvement Committee**

1.INTRODUCTION

Technology has become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people have an entitlement to safe internet access at all times.

This Online Safety Policy is designed to help to ensure safe and appropriate use and support children to be able to identify and manage risks associated with online activity. The use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and as such this Online Safety Policy is used in conjunction with other school safeguarding policies e.g. Child Protection, Behaviour and Anti-Bullying.

As it is impossible to eliminate all risk completely it is essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

2.SCOPE OF THE POLICY

This policy applies to all members of the school community including staff, pupils, governors, volunteers, parents / carers, visitors who have access to and are users of school ICT systems, both in and out of school. The school will deal with online safety incidents in the same way as associated safeguarding/behaviour/bullying incidents and will, where it becomes aware, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

3.SCHEDULE FOR DEVELOPMENT / MONITORING / REVIEW

The implementation of this Online Safety Policy will be monitored by the Computing Lead. Monitoring will take place continuously. The Governing Body will receive a report on the implementation of the Online Policy (which will include anonymous details of Online incidents) from the Computing Lead at least annually. The Online Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

4.ROLES AND RESPONSIBILITIES

Governors

Governors are responsible for the approval and adoption of the Online Safety Policy and for reviewing the effectiveness of the policy. They should be kept up to date with any online safeguarding incidents and follow them up using the correct procedures. Governors should keep up to date with new online safety training and legislation.

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 Computing Lead.
- The Headteacher and Deputy Headteacher 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 is responsible for ensuring that the Computing Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues.
- The Headteacher 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, all issues will be brought to the attention of the Headteacher.

Computing lead

- 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.
- Meets with the Headteacher and / or online safety Governor to discuss any current issues, review incident logs.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher or Computing Lead for investigation
- all digital communications with pupils / parents / carers are on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and Acceptable Use Agreement

Designated Safeguarding Lead

Designated Safeguarding Officers should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- sexting

Pupils

- Are responsible for using the school computing systems in accordance with the Pupil 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
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

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. The school will seek help parents understand these issues through newsletters, letters, the website and other means of communication. Parents and carers will be encouraged to support the school 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 has been allowed)
- messages sent home that are shared online

5.CURRICULUM

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of Computing across the curriculum:

- Where pupils are allowed to search the internet independently in lessons, e.g. using search engines, 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, pupils 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 Network Manager (OneIT) 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.
- Pupils 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

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

6.EDUCATION & TRAINING

- All staff should receive online safety current updates and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Computing Lead will receive regular updates through attendance at external training events, by signing up for regular email updates 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 meetings.
- The Computing Lead will provide advice / guidance / training to individuals as required.

In the case of remote learning, staff should be aware of the following:

- Laptops provided by the school should be used
- Teams should be used for video calling and messaging.
- Staff should ensure that their background is blurred and/or all objects deemed inappropriate be removed from the background.
- Work should be provided for children who cannot attend school through the SeeSaw app.
- Laptops provided by the school should only be used for work activities. These devices will be monitored by OneIT.

7.USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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 pupils 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.
- Staff 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.
- 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. 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 pupils.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupils' work can only be published with the permission of the pupil and parents or carers.

8.DATA PROTECTION

When personal data is stored on any portable computer system, memory stick, or any other removable media or device (including phones), the school strongly recommends that staff:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices.
- Ensure that they are properly "logged-off" at the end of any session or 'remote' session.
- Transfer data using encryption and secure password protected devices where possible.
- Access sensitive / personal data from home using their 'remote' login rather than copying data onto unprotected memory sticks or external hard drives.
- Securely delete data from any device once it has been transferred or its use is complete.
- Report any loss or theft of a removable / portable device containing sensitive / personal data to the Computing Lead as soon as possible.

9.TECHNICAL – INFRASTRUCTURE / EQUIPMENT, FILTERING AND MONITORING

The school will be responsible for ensuring that the school 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 need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

School technical systems will be managed in ways that ensure that the recommended technical requirements.

- There will be regular reviews and audits of the safety and security of school technical systems –these responsibilities are delegated to the academy IT Service Provider – ONE IT.
- 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 (at KS2 and above) will be provided with a username and secure password
- Users are responsible for the security of their username and password
- The "administrator" passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.

- An agreed policy of only using encrypted memory sticks is in place regarding the use of removable media by users on school devices.

10.UNSUITABLE / INAPPROPRIATE ACTIVITIES

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section are inappropriate in a school context and that users should not engage in the activities as defined below in / or outside the school when using school equipment or systems. Staff found to engage in these activities will be subject to investigation which could lead to criminal and/or disciplinary procedures including dismissal. The school policy therefore prohibits such usage:

- Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978.
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008.
- Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986.
- Pornography.
- Promotion of any kind of discrimination.
- Threatening behaviour, including promotion of physical violence or mental harm.
- Promotion of extremism or terrorism.
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.
- Using school systems to run a private business.
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Infringing copyright.
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords).
- Creating or propagating computer viruses or other harmful files.
- Unfair usage (downloading / uploading large files that hinders others in their use of the internet).
- On-line gaming (educational or non-educational).
- On-line gambling.
- On-line shopping / commerce for personal – non school - purposes

11.RESPONDING TO INCIDENTS OF MISUSE

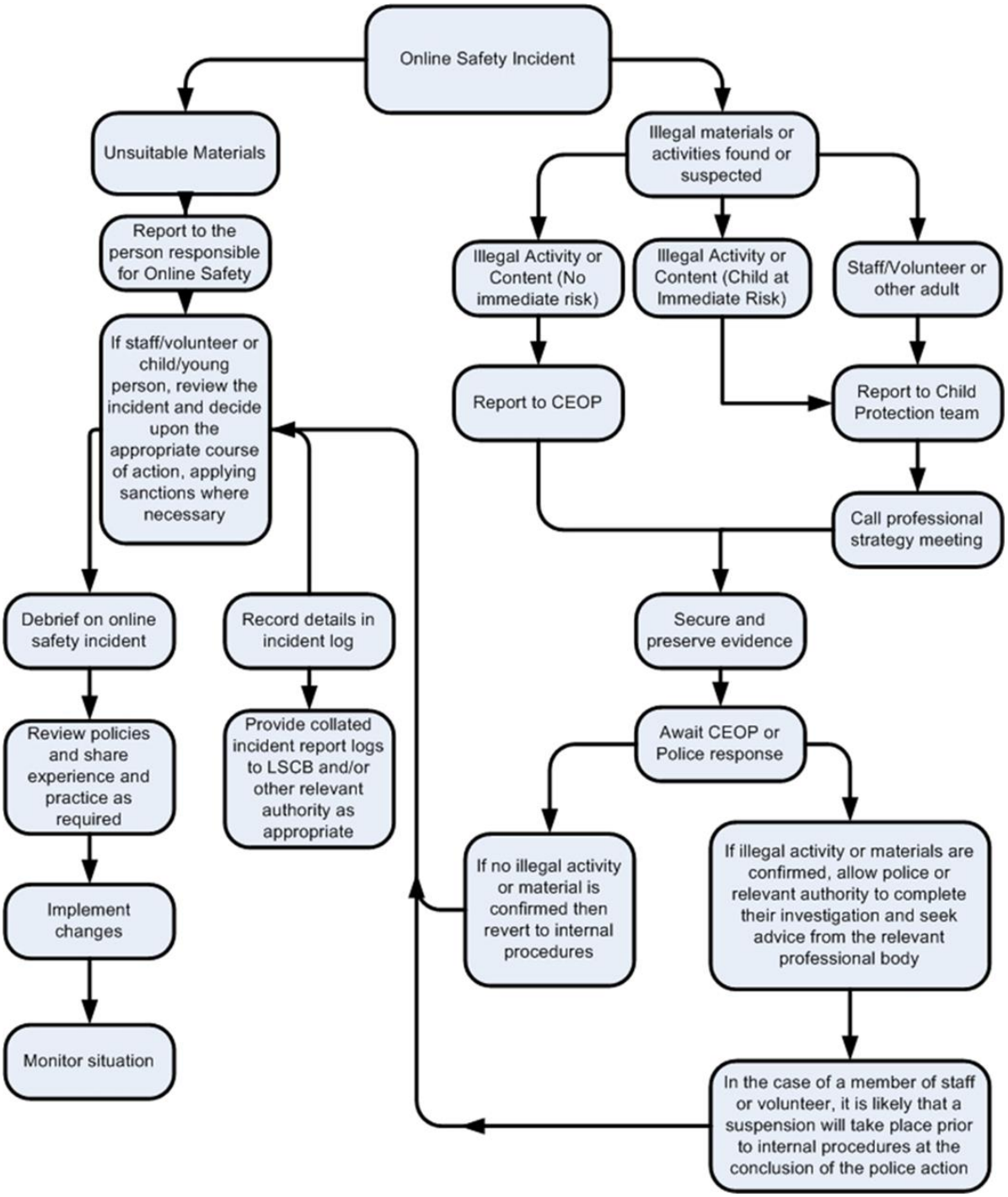
This guidance is intended for use when leaders need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

School Actions & Sanctions

When the school needs to deal with incidents that involve inappropriate misuse of systems (see example incidents below), both staff and/or pupils, 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 and the action/sanction selected in each case will be dealt with through normal behaviour / disciplinary procedures. See appendix 1 for examples of potential misuse.

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 and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

APPENDIX 1

PUPILS INCIDENTS

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
- Unauthorised use of non-educational sites during lessons.
- Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device.
- Unauthorised / inappropriate use of social media / messaging apps / personal email.
- Unauthorised downloading or uploading of files.
- Allowing others to access school network by sharing username and passwords.
- Attempting to access or accessing the school network, using another student's / pupil's account.
- Attempting to access or accessing the school network, using the account of a member of staff.
- Corrupting or destroying the data of other users.
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature.
- Continued infringements of the above, following previous warnings or sanctions.
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.
- Using proxy sites or other means to subvert the school's filtering system.
- Accidentally accessing offensive or pornographic material and failing to report the incident.
- Deliberately accessing or trying to access offensive or pornographic material.
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.

STAFF INCIDENTS

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
- Inappropriate personal use of the internet / social media / personal email.
- Unauthorised downloading or uploading of files.
- Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.
- Careless use of personal data e.g. holding or transferring data in an insecure manner.
- Deliberate actions to breach data protection or network security rules.
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature.
- Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils.
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.
- Using proxy sites or other means to subvert the school's filtering system.
- Accidentally accessing offensive or pornographic material and failing to report the incident.
- Deliberately accessing or trying to access offensive or pornographic material.
- Breaching copyright or licensing regulations.
- Continued infringements of the above, following previous warnings or sanctions.