Approved: Autumn 2020
Review: Autumn 2023

ONLINE SAFETY POLICY

OVERVIEW

This policy applies to all members of the school community (including staff, pupils, parents/carers and visitors. This Online Safety policy is part of our wider safeguarding agenda and outlines how we will ensure our school community is prepared to deal with the safety challenges that the use of technology brings. It is the duty of all members of the school community to be aware of Online Safety at all times, to know the required procedures and to act on them.

This policy should be read in conjunction with the following:

- Child Protection and Safeguarding Children/Staff Code of Conduct
- Social Media policy
- Mobile Phone and Handheld Devices policy
- Recording and Use of Images of Pupils policy
- Attitude, Behaviour and Discipline policy
- Anti-Bullying policy
- Acceptable Use of ICT policy

RATIONALE

Research has proven that the use of technology brings enormous benefits to learning and teaching and helps raise educational standards. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective online Safety policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

It is the duty of the school to ensure that every child in our care is safe. All staff have a responsibility to support Online Safety practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach Online Safety policies. Online Safety is a partnership concern and is not limited to school premises, school equipment or the school day. Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyberbullying will be dealt with through the school's Attitude, Behaviour and Discipline policy.

STRATEGIES

Roles and responsibilities

The Governor Body will ensure that:

- The Safeguarding team are responsible for taking the lead on Online Safety within the school.
- The Safeguarding/Child Protection governor will ensure Online Safety is embedded in all child protection practice and will check the school Online Safety policy as needed.
- Procedures are in place for dealing with breaches of Online Safety and security and are in line with Local Authority procedures.
- All staff and volunteers have access to appropriate ICT training.

The Head Teacher will ensure that:

- There is an overview of Online Safety (as part of the wider remit of Safeguarding)
- Online Safety is promoted across the curriculum and has an awareness of how this is being developed and linked within the school development plan.
- All staff should be included in Online Safety training and that staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- Ensure that any misuse or incident has been dealt with appropriately according to policy and procedure,
- Liaise with the school's IT Network manager to ensure all computers/laptops in school have adequate filtering levels.
- Liaise with the PSHE, ICT and Child Protection leads so that policies and procedures are up to date to take account of any emerging issues and technologies
- Work alongside the IT Network Manager to ensure there is appropriate and up to date anti-virus software and anti-spyware on the network stand a- lone PCs and teacher/child laptops and this is reviewed and updated on a regular basis

The Designated Member of Staff for Online Safety will:

- Act as the first point of contact with regards to breaches in Online Safety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff and volunteers on Online Safety.
- Ensure that all staff and volunteers have received and signed a copy of the school's Acceptable Use of ICT policy document.
- Ensure that all staff and volunteers understand and are aware of the school's Online Safety Policy.
- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Regularly check files on the school's network.

Staff and adults will:

- Ensure that they know who the designated persons are for Safeguarding so that any misuse or incident can be reported which involve a child.

- Be familiar with the Acceptable Use of ICT, Anti-Bullying, Attitude, Behaviour & Discipline and other relevant policies so that in the event of misuse or allegation, the correct procedures can be followed.
- Ensure that children are protected and supported in their use of online technology so that they know how to use it in a safe and responsible manner.
- Be up to date with online safety knowledge that is appropriate for the age group they work with and reinforce this through the curriculum.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998.

Pupils will be:

- Responsible for following the school's Acceptable Use of ICT rules whilst within school as agreed with their class teacher. These rules will be displayed in the classrooms and other places where computer/laptops are being used.
- Taught to use the internet in a safe and responsible manner through ICT, PSHE and other curriculum lessons
- Taught to tell an adult about any inappropriate material or contact from someone they do not know straight away (using age appropriate methods for teaching)

MANAGING THE INFRASTRUCTURE

The Online Safety Co-ordinator will liaise with the office manager, the IT network manager and Sefton LA to ensure that the systems in place at school are rigid and current. The network manager will review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed.

Wide Area Network (WAN) security issues include:

- All Internet connections must be arranged by the IT network manager in order to ensure compliance with our school's policies and procedures.

MANAGEMENT OF THE SCHOOL'S INFORMATION SYSTEMS

The security of the school information systems and users will be reviewed regularly.

Virus protection will be updated regularly.

- Portable media is not permitted unless authorized by the network manager.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Software cannot be installed or downloaded without administrator rights.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/ IT network manager will review system capacity regularly.

USING THE INTERNET TO ENHANCE LEARNING

The internet is a part of the statutory curriculum and a necessary tool of staff and children and benefits education by allowing access to worldwide educational resources including art galleries, museums as well as enabling access to specialist information. The internet also supports the professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with the Local Authority and Department for Education.

Pupils will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques and encouraged to question the information.

Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported firstly immediately to the Head and to the IT network manager.

The school's Internet access is planned and designed to enhance and extend education. Pupils will be taught what Internet use is acceptable and what is not and give clear objectives for Internet use. Pupils are supervised during internet access and are encouraged to report inappropriate material as soon as possible to a member of staff.

The schools will ensure that the copying and subsequent use of Internet derived material by staff and pupils complies with copyright law.

- Access levels reflect the curriculum requirements and age of pupils.
- Staff guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

FILTERING CONTENT

Levels of Internet access and supervision are rigid in accordance with the limits set by Schools Broadband (Talk Straight). The Online Safety Co-ordinator will work with the school's network manager to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL must be reported to the Online Safety Coordinator and immediate blocking will take place via the IT network manager. The school's broadband access includes filtering appropriate to the age and maturity of pupils. Our filtering system used in school is Newsweeper. Our ICT network manager has overall administration.

MANAGING EMAIL

Email is an essential means of communication for staff. Directed email use can bring significant educational benefits and interesting projects between schools in neighboring communities and worldwide.

Staff are provided with an email address as part of their induction process. The Head Teacher is responsible for requesting the email address to be set up by the school's IT network manager. On no account should staff provide a pupil with their personal or school email address. Staff emails may be passed to parents as a form of communication.

Pupils must not reveal personal details of themselves or others in any communication.

MANAGING WEBSITE CONTENT

Still and moving images and sounds add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless, the security of staff and pupils is paramount. The publishing of pupils' full names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown. Pupils in photographs should, of course, be appropriately clothed.

Please refer to the **Use of Images of Pupils policy.**

PHOTOGRAPHIC, VIDEO AND AUDIO EQUIPMENT

It is not appropriate to photograph or video near the vicinity of toilets or in areas when children are changing.

Staff may use photographic or video equipment to record school visits and appropriate curriculum activities.

Webcam use will be appropriately supervised for the age of the pupil.

Please refer to the **Use of Images of Pupils policy.**

MANAGING SOCIAL NETWORKING

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

For responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content.

All staff should be aware of the potential risks of using social networking sites in line with the school's **Social Network policy**. They should be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chat rooms, instant messenger.

The school will not allow access to social media or social networking sites to either staff or pupils whilst onsite.

Pupils are advised, during safe internet lessons and Online Safety training sessions at the never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends/family, specific interests and clubs etc.

- Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.
- Pupils are to contact a member of staff if they are at all concerned about incidents or problems associated with the internet or mobile phones.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications at home. Pupils should be encouraged to invite known friends only and deny access to others by making profiles private.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

THE USE OF MOBILE PHONES AND HANDHELD DEVICES

Schools should keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. For instance, text messaging via mobile phones is a frequent activity for many pupils and families; currently we use texting to ensure parents are informed about emergency closures and meetings that they are expected to attend.

Please refer to the school's **Mobile Phone and Handheld Devices policy.**

PROTECTION OF PERSONAL DATA

The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date

- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

CYBERBULLYING

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

Cyberbullying (along with all forms of bullying) will not be tolerated in school.

Full details are set out in the school's **Attitude, Behavior and Discipline policy**.

There will be clear procedures in place to support anyone affected by Cyberbullying-

please refer to the Attitude, Behavior and Discipline policy for sanctions and procedures.

INTRODUCING THE POLICY TO PUPILS

Rules for internet access and Acceptable Use will be posted in all rooms where computers or laptops are used.

Pupils will be instructed in responsible and safe use before being allowed access to the internet and will be reminded of the rules and risks before any lesson using the internet.

Pupils will be reminded that internet use will be closely monitored and that misuse will be dealt with appropriately.

SUPPORT OF PARENTS

Parents/carers will be informed of the school's Online Safety policy and the Acceptable Use of ICT policy, which will be accessed on the school website.

A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting Online Safety at other attended events e.g Online Safety talks, newsletters etc.

Any issues concerning the internet/online safety will be handled sensitively to inform parents/carers without undue alarm.

Advice on filtering systems and appropriate educational and leisure activities will be made available to parents/carers via the school website.

Information and guidance for parents on Online Safety will be made available to parents in a variety of formats.

Interested parents will be referred to organisations listed in section "Online Safety Contacts and References."

DEALING WITH COMPLAINTS

Staff, pupils, volunteers and parents/carers must know how and where to report incidents. Concerns related to Safeguarding issues must be dealt with through the school's Safeguarding policy and referred to the Safeguarding team.

The school's designated person for online safety will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be

reported to the Head Teacher immediately.

Sanctions for misuse by children may include any or all of the following:

- Informing parents/carers
- A ban on access to the internet in school
- Exclusion from school
- Referral to the police

REVIEW

This policy will be reviewed every 3 years by the Safeguarding Team and the Governing Body.

APPENDIX 1

Online-Safety Contacts and References

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

Childline: *www.childline.org.uk*

Childnet: *www.childnet.com*

Click Clever Click Safe Campaign: *http://clickcleverclicksafe.direct.gov.uk*

Cybermentors: *www.cybermentors.org.uk*

Digizen: *www.digizen.org.uk*

Internet Watch Foundation: *www.iwf.org.uk*

Teach Today: *http://en.teachtoday.eu*

Think U Know website: *www.thinkuknow.co.uk*

Virtual Global Taskforce — Report Abuse: *www.virtualglobaltaskforce.com*

NSPCC Parental Controls:

https://www.nspcc.org.uk/keeping-children-safe/online-safety/parental-controls/

NSPCC Inappropriate and Explicit content:

https://www.nspcc.org.uk/keeping-children-safe/online-safety/inappropriate-explicit-content/