Local Arrangements for Online Safety at Sutton Park Primary School

(to be read in conjunction with CRST Online Safety Policy)

Date ratified	04/12/2025
Next review	December 2026
Signed by Chair of Governors	K E Maynerd

Rationale

The purpose of this document is to support the Central Region Schools Trust online safety policy. It will aim to:

- set out the key principles expected of all members of our school community with respect to the use of computing and ICT-based technologies;
- safeguard and protect our children and staff;
- assist our school staff when working with children, to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice;
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use;
- have clear structures to deal with online abuse such as cyber-bullying which are cross referenced with other school policies;
- ensure that all members of our school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken;
- minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (Internet or gaming)
- Peer on peer abuse including sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (care or consideration for intellectual property and ownership - such as music and film)

Education and curriculum

School e-safety curriculum

This school has a clear, progressive e-safety education programme as part of the computing curriculum and also the PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and through this aims to:

- plan careful Internet use to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- teach pupils about their responsibilities through an end-user acceptable use policy (AUP) which every pupil will be reminded of at the beginning of each lesson technology is used.
- ensure staff model safe and responsible behaviour in their own use of technology during lessons;
- ensure that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;

- ensure that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include risks in pop-ups; buying on-line; on-line gaming / gambling.

Staff and governor training
Sutton Park Primary School:
- ensures staff and governors know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Provides all teaching staff with an encrypted USB stick to ensure data is secure.
- makes regular training available to staff on e-safety issues and the school's e-safety education program;
- provides all new staff (including those on university/college placement and work experience) with information and guidance on the online safety policy and the school's acceptable use policy (AUP).

Parent awareness and training
Sutton Park Primary School provides a programme of advice, guidance and training for parents, including:
- information leaflets, in-school newsletters, information and advice on the school web site;
- suggestions for safe Internet use at home;
- provision of information about national support sites for parents.

Expected conduct and incident management
Expected conduct
At Sutton Park Primary School, all users:
- are responsible for using the school systems in accordance with the relevant school policies;
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences;
- 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 e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school;
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking and/or use of images and on cyber-bullying.

Staff are responsible for reading the Trust Online Safety Policy, the local arrangements for online safety, and using the school computing systems accordingly, including the use of mobile phones, and handheld devices.

Pupils should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/carers should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident management
In this school and in line with the Central Region Schools Trust Online Safety Policy:
- there is strict monitoring (through the use of our online monitoring software 'SENSO') application of the online safety policy and a differentiated and appropriate range of sanctions), though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions;
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (e.g. the Local Authority)

- monitoring and reporting of e-safety incidents takes place and contributes to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders and governors
- parents/carers are informed of e-safety incidents involving pupils for whom they are responsible. Where possible, this would happen on the day of the incident as it is a crucial part of our safeguarding process.
- Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

Password policy
- At Sutton Park Primary School, we make it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- All pupils have their own unique username and passwords.

Social networking
School staff will ensure that in private use:
- no reference should be made in social media to pupils, parents / carers or school staff
- they do not engage in online discussion on personal matters relating to the school community
- personal opinions should not be attributed to the school or Local Authority
- they ensure their use of social networking sites is respectable and appropriate at all times
- personal profiles do not identify their place of work
- they do not use a work email to sign up to non-work related web-accounts
- they do not have contact with students using social media
- they do not add pupils as friends or respond to friend requests from pupils
- secure and suitable strength passwords are used
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Equipment and Digital Content
Personal mobile phones and mobile devices
- Mobile phones brought into school are entirely at the staff member, pupils', parents' or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Pupil mobile phones can be brought into school, but are safely secured by the class teacher during the day. All staff and visitors are requested to keep their phones on silent and use them only during break times in staff work rooms and outside of the school premises.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

Staff use of devices
- Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional or personal capacity.
- Staff will use a school phone where contact with pupils, parents or carers is required.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

- If a member of staff breaches the school policy then disciplinary action may be taken. Staff members may be required to use a mobile phone for school duties, for instance in case of emergency during off-site activities.

Digital images and video
In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

  These Local Arrangements will be reviewed in a timely manner in accordance with the Central Region Schools Trust Online Safety Policy.

Appendix A

Role	Key Responsibilities
Senior Leadership Team	• To take overall responsibility for e-safety provision. • To take overall responsibility for data and data security. • To ensure the school uses an approved, filtered Internet service, which complies with current statutory requirements. • To be responsible for ensuring that all teaching and non-teaching staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the e-safety lead. • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures.
Assistant Principal Online Safety Lead Computing Lead	• To take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents. • To promote an awareness and commitment to e-safeguarding throughout the school community. • To ensure that e-safety education is embedded across the curriculum. • To liaise with Academy technical staff on the latest developments. • To communicate regularly with SLT and the designated e-safety governor / governing body committee to discuss current issues, review incident logs and filtering. • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident. • To ensure that E Safety is continually monitored via SENSO. • To facilitate training and advice for all staff. • To liaise with the local authority (LA) and other relevant agencies. • To be regularly updated regarding e-safety issues and legislation, 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 and use of social media. • To oversee the delivery of the e-safety element of the computing curriculum. • To liaise with the PSHE lead on a regular basis
Governors	• To ensure that the school follows all current e-safety advice to keep the children and staff safe. • To approve the 'Local Arrangements for Online Safety' document and review the effectiveness of this. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities.
Network manager / technician	• To report any e-safety related issues that arises, to the e-safety lead. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • To ensure that provision exists for misuse detection and malicious attack eg keeping virus protection up to date. • To ensure the security of the school computer system. • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices. • To ensure the school's policy on web filtering is applied and updated on a regular basis. • To ensure that he/she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

Role	Key Responsibilities
	• To ensure that the use of the network / Virtual Learning Environment / remote access / e-mail is regularly monitored in order that any misuse / attempted misuse can be reported to the e-safety lead/SLT for investigation / action / sanction . • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities. • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant). • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	• To read, understand and help promote the Central Region Schools Trust Online Safety Policy and the Local Arrangements for Online Safety document. • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices. • To report any suspected misuse or problem to the e-safety lead. • To maintain an awareness of current e-safety issues and guidance e.g. through CPD. • To model safe, responsible and professional behaviours in their own use of technology. • To ensure that any digital communications with pupils should be on a professional level and only through school based systems (Seesaw), and never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand and adhere to the pupil acceptable use policy. • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • Understand the importance of reporting abuse, misuse or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school arrangements on the use of mobile phones, digital cameras and hand held devices. • To know and understand school arrangements on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's Local Arrangements for Online Safety document covers their actions out of school, if related to their membership of the school. • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home. • To help the school in the creation/ review of online safety documents. (PLT)
Parents/carers	• To support the school in promoting e-safety and endorse the parents' acceptable use agreement which includes the pupils' use of the internet and the school's use of photographic and video images. • To read, understand and promote the school pupil acceptable use agreement with their children. • To access the school website / on-line student / pupil records in accordance with the relevant school acceptable use policy. • To consult with the school if they have any concerns about their children's use of technology.
External groups	• Any external individual / organisation will be made aware of the school's acceptable use policy (AUP) prior to using any equipment or the internet within school.

Sutton Park Primary School
AUP for learners in KS1

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me
  feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger
- not damage or misuse any IT equipment.

Anything I do on the computer may be seen by someone else.

I am aware of the CEOP report button and know when to use it.

I understand that my online search history and computer activity are monitored for my safety.

Signed _____ ***Date*** _____

Sutton Park Primary School
AUP for learners in KS2.

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only use, move and share personal data securely
- only visit sites which are appropriate
- work in collaboration only with people my school has approved and will deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not use my own mobile device in school unless I am given permission
- only give my mobile phone number to friends I know in real life and trust
- only email people I know or approved by my school
- only use email which has been provided by school
- discuss and agree my use of a social networking site with a responsible adult at home before joining
- always follow the terms and conditions when using a site
- always keep my personal details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- not damage or misuse any IT equipment.

I am aware of the CEOP report button and know when to use it.

I understand that my online search history and computer activity are monitored for my safety.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Signed _____ Date _____