Sutton CE (VC) Primary School

E-Safety Policy

Version 2019v1

Approved by Governors March 2019
Approved by staff March 2019

Contents

- The background to this policy
- Rationale
- The E-Safety Curriculum
- Continued Professional Development
- Monitoring, and preventing e-safety incidents
- Responding to e-safety incidents
- Appendices (including AUPs)

Background to this policy:

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school in relation to e-safety, including:

- The policies and practice embedded in our school and followed by the who school community
- The infrastructure and how it is set up to keep pupils safe online, including monitoring, and preventing and responding to e-safety incidents
- A progressive, age appropriate e-safety curriculum for all pupils

Online safety in schools is primarily a safeguarding and not a computing / technology one. Therefore this policy should be viewed alongside other Safeguarding policies and approaches including, but not limited to:

- Professional boundaries in relation to your personal internet use and social networking online – advice to staff (LSCB)
- Safeguarding and Child Protection
- Personal Social and Health Education (PSHE)
- Safer Working Practices
- Data Protection Policy
- Anti-Bullying Policy
- School Complaints Procedure
- Cambridgeshire Progression in Computing Capability Materials
- Whistle Blowing Policy

This policy must be read alongside the staff and pupil Acceptable Use Policies attached as appendices. These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology.

- The development of our safety policy involved:
  The Headteacher
  The Designated Person for Child Protection
  The Computing Subject Leader
  Cambridgeshire Local Authority Advisor (Cambridgeshire Education ICT Service)
  The governor responsible for Safeguarding

- This policy may also be partly reviewed and / or adapted in response to specific e-safety incidents or developments in the school's use of technology. It has been shared with all staff via email and a staff meeting and is readily available on the school network and website.

- All staff must be familiar with this policy and all staff and pupils must sign the relevant Acceptable Use Policy before being allowed to access school's systems (see appendices). As E-safety is an important part of strategic leadership within the school, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Person for Child Protection and governors.

Rationale:

At Sutton CE (VC) Primary School we believe that the use of technology in school brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the use of these new technologies can put young people at risk within and outside the school.

The risks they may face can broadly be categorised into the '3 C's' **Contact**, **Content** and **Conduct** (Livingston and Haddon) and may include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images
- 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
- Cyber-bullying
- 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.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. E-Safety issues can also affect adults who work or are associated with the school and this will be referenced in more detail later in this policy.

Technologies regularly used by pupils and staff include:

Staff:

- Staff laptops and also desktops in the office and ICT Suite including staff level internet access, server access and access to MIS systems.
- Some staff have access to MIS systems from home via a secure logon and keyfob. Staff laptops can also be used at home in accordance with the staff AUP.
- Class cameras and other peripherals such as visualisers and Interactive Whiteboards
- i-pads (each teacher has a class i-pad which is treated similarly to a staff laptop – access to the ability to download apps is limited)

Pupils:

- Curriculum laptops in the two laptop trolleys we have including filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources (Beebots, control equipment, class cameras etc.)
- i-pads – (ability to download apps on these is impossible without the password)

Where the school changes the use of existing technology or introduces new technologies which may pose risks to pupils' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

The online safety Curriculum:

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or

situations which make them feel uncomfortable. The need for a progressive, age appropriate e-safety curriculum is clearly documented in the National Curriculum for Computing which states that:

- **At KS1:** use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- **At KS2:** use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

At Sutton CE (VC) Primary School we believe that a comprehensive programme of e-safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials including the ACE (Accredited Competence in E-safety) scheme of work and is linked to our online learning platform, Starz+.
- Our programme for e-safety education is evidenced in teachers' planning either as discrete or embedded activities.
- Key online safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in discussion forums.

Continued Professional Development:

- Staff at Sutton CE (VC) Primary School receive up-to-date information and training on e-Safety issues in the form of staff meetings and updates from Computing Subject Leader, as well as training from external providers where appropriate.
- Nominated members of staff receive more in depth online safety training to support them in keeping up to date and reviewing the school's approach, policies and practice.
- New staff receive information on the school's acceptable use policy as part of their induction, including advice on Protecting their Professional Reputation Online.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.

School website:

Schools are required to publish certain information online – which in practice means you must have a school website. You are not however required to develop a website policy but sometimes the boundaries of responsibility for setting up, maintaining and ownership of the content are blurred and this can lead to difficulty.

The main purpose of our school website is to provide information. Our school website will not only tell the world that our school exists, but it will provide information our pupils and parents, promote the school to prospective ones and publish the statutory information required by the Department for Education.

In conjunction with a range of online services, a school website can be used to showcase examples of pupils' work - in words, pictures, sound or movie clips - and can share resources for teaching and learning both within the school and with colleagues elsewhere.

Under safeguarding responsibilities, it is the duty of a school to ensure that every child in their care is safe, and the same principles should apply to the virtual presence of a school as it would apply to its physical surroundings. Headteachers and the Governing Body should therefore take on the responsibility to ensure that no individual child can be identified or contacted either via, or as a result of, a visitor using the school website.

The school should establish clear policies to ensure that its website is maintained, is effective, and does not compromise the safety of the pupils or staff.

Monitoring, and averting e-safety incidents:

The school keeps children safe when using online technologies through a combination of e-safety education, filtering and monitoring children's online activity and reporting incidents, including following Child protection procedures where appropriate.

The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both the East of England Broadband Network (E2BN) and the Local Authority's Education ICT Service. Safeguards built into the school's infrastructure include:

- Secure, private CPSN provided internet connection to each school with a direct link to the National Education Network.
- Managed firewalling running Unified threat management (UTM) that provides Restrictions on download of software, apps and file types from known compromised sites.
- Base line and optional enhanced filtering.
- Optional SSL decryption available on web traffic to allow for greater visibility of sites being accessed and requested.
- Antivirus package provided as part of CPSN Connection.
- Email system for all school staff with direct internal routes to the council for trusted email communications.

- Wireless networks installed by The ICT Service are encrypted to industry best practice standards and the wireless key should be kept securely by the school office.
- Staff also monitor pupils' use of technology and, specifically, the internet.

Staff also monitor pupil's use of technology and, specifically, their activity online

- Pupils' use of online services (including the World Wide Web) are supervised in school at all times.
- Staff are also able to monitor pupils' activity in the Starz+ learning platform, allowing them to identify inappropriate or concerning online behaviour, as well as respond to reports of any such behaviour from pupils or parents.

A system of staff and pupil passwords is in place to enable appropriate access to the school network.

- All members of staff have individual, password protected logins to the school network.
- Visitors to the school can access part of the network using a generic visitor login and password.
- The school's network can either be accessed using a wired or wireless connection. However, the wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office.
- School staff and pupils are not permitted to connect personal devices to the school's wireless network and a guest wireless key is issued to visitors on a case by case basis.

Whilst we recognise that it is impossible to totally eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks as much as possible.

Responding to E-Safety Incidents:

It is important that all members of staff - teaching and non-teaching – are aware of how to respond if an e-safety incident occurs or they suspect a child is at risk through their use of technology.

- Staff responses to e-safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.
- If an e-safety incident occurs, Sutton CE (VC) Primary School will follow its agreed procedures for responding including internal sanctions and involvement of parents (this may include the deactivation of accounts or restricted access to systems as per the school's AUPs – see appendix).

In addition, the Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents

which may take place outside of the school but has an impact within the school community.

- With this in mind, the Headteacher may decide to apply the sanctions and / or procedures in the relevant AUP to incidents which occur outside of schools if s/he deems it appropriate.

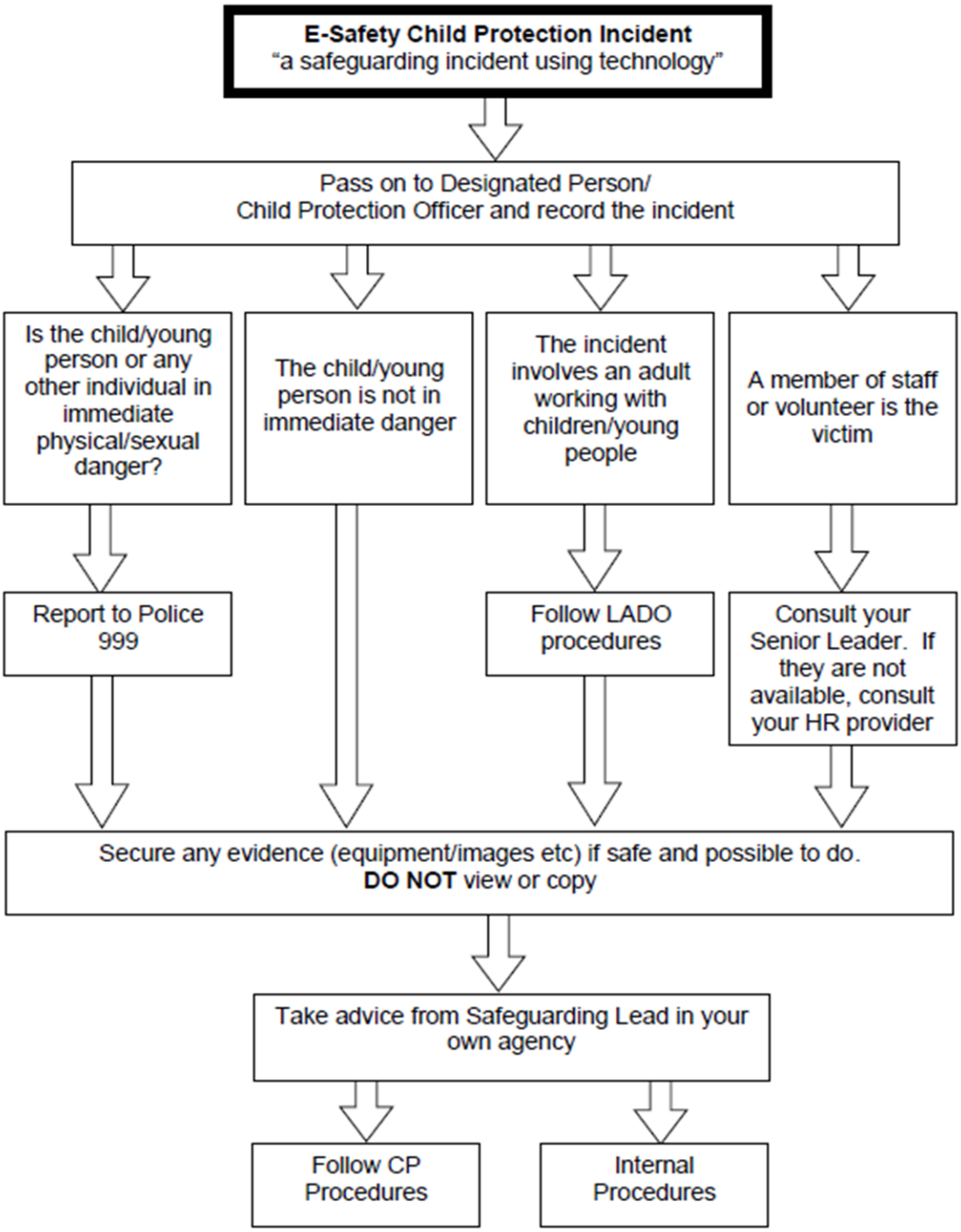
The Education Act 2011 gives school staff the powers, in some circumstances to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.

However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk where it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern with parents (where appropriate) before taking any further action.

NB: In our school, the likelihood of these types of instances occurring are already reduced as we don't allow pupils to use personal devices in school.

Where the school suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed. This process is illustrated in the diagram below.

You come across a child protection concern involving technology …



Sutton CE (VC) Primary School Staff Acceptable Use Policy (AUP)

I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities. I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's management information system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority. I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.

I will

- only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- use the approved, secure email system(s) for all school business with pupils or parents/carers and only communicate with them on appropriate school business.
- ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- report any accidental access to, or receipt of inappropriate materials, or filtering breach to the eSafety Co-ordinator, Designated Person for Child Protection or Headteacher, as appropriate
- use the school's Learning Platform in accordance with school and Local Authority advice.
- ensure that any private social networking sites / blogs etc that I create or actively contribute to do not compromise and are not confused with my professional role.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- will promote e-safety with pupils in my care and will help them to develop a responsible attitude to their use of ICT.

I will not

- share or reveal my password(s) to anyone.
- allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- engage in any online activity that may compromise my professional responsibilities
- allow children to logon using my username and password
- browse, download or send material that could be considered offensive, illegal or discriminatory.
- download any software or resources from the Internet that can compromise the network, or are not adequately licensed.

- connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software.
- use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and
- I will not store images at home without permission.

I understand that once I sign this document, failure to comply with this agreement could lead to disciplinary action.

Name: **Signed:** **Date:**

Key Stage 2 Acceptable Use Policy

- ICT equipment and tools (including computers, cameras, Starz etc.) for schoolwork and homework. If I need to use the school's computers for anything else, I will ask for permission first.

- I will only use the Internet if a teacher or teaching assistant is in the room with me.

- I will only delete my own files only if my teacher gives me permission to delete them. I will
not look at other people's files without their permission.

- I will keep my passwords secret and tell my teacher if I think someone else knows them.

- I will only use my class e-mail address or my own school e-mail address when e-mailing.

- I will only open e-mail attachments from people who I know or my teacher has approved. If I am unsure about an attachment or e-mail, I will ask my teacher for help.

- I will make sure that all communication with other children and adults is responsible, polite and sensible.

- I will not give my own personal details such as surname, phone number or home address or any other personal details that could be used to identify me, my friends or my family. If I have to use an online name I will make one up!

- I will never post photographs or video clips of people I know without permission and never include names with photographs or videos.

- I will never arrange to meet someone I have only ever previously met online. It could be dangerous.

- I will not deliberately look for, save or send anything that could be unpleasant or upsetting. If I find anything via Internet, e-mail or mobile phone that is upsetting or makes me feel uncomfortable, I will tell a teacher or responsible adult.

- I will be responsible for my behaviour because I know that these rules are there to keep me safe. If I break these rules I know I will have to deal with consequences.

Key Stage 1 Acceptable Use Policy

- I will use the school's ICT equipment and tools (including computers, cameras, Starz etc.) for schoolwork and homework. If I need to use the school's computers for anything else, I will ask for permission first.
- I will only use the internet and email when an adult is nearby.
- I will keep my passwords 'Top Secret' and tell my teacher if I think someone else knows them.
- I will only use my school e-mail address when e-mailing.
- I will ask an adult before opening an email from someone I don't know.
- I will not share details about myself such as surname, phone number or home address.
- I will ask if I need to look at other peoples' work on the computer.
- I will only send friendly and polite messages.
- I will ask my teacher before using photos or video.
- If I see something on a screen which upsets me, I will always tell an adult.