



Sherrier C of E Primary School

E-SAFETY POLICY

September 2021

Date for next review September 2022

E-safety Policy

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors..

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body and/or parents.

Safeguarding is a serious matter; at Sherrier C of E Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the SafeICT School website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. All students will be made aware of the key points of this policy and the Students Acceptable Use Policy and the beginning of each school year. Students will be required to sign a permission slip to show acceptance of the terms and conditions. Only after this will Sherrier permit students access to schools technology including the internet.

Policy Governance (Roles & Responsibilities)

Note: This section notes the roles and responsibilities of each person/body.

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- The Safeguarding governor to have overall responsibility for the governance of e-safety at the school who will:
 - Keep up to date with emerging risks and threats through technology use.
 - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
 - Provide feedback at full governors meetings.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer, as indicated below.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

e-Safety Officer

The day-to-day duty of e-Safety Officer is devolved to *Rebecca Weed*

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log (Appendix A); ensure staff know what to report and ensure the appropriate audit trail.

- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Note: At Sherrier technical support is outsourced to Leamis. This policy will be brought to their attention and they will sign it, in line with school practice.

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
 - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
 - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
 - Any e-safety technical solutions such as Internet filtering are operating correctly.
 - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
 - Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters and will be requested to be changed termly.
 - The IT System Administrator password is to be changed on a half-termly basis.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

e-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, school newsletters, website updates and social networking updates. The school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs to have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technology

Sherrier C of E Primary School uses a range of devices including PC's, laptops and iPads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use Openhive webshield software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Computing Coordinator, e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use Openhive webshield software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Monitoring- we use Future Digital Footprint software that monitors all activity on the computers in school. This monitoring software alerts staff of any online harmful behavior or content. It also creates a screenshot of any harmful activity allowing teachers to assess context and severity.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

Passwords – all staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change on a termly basis or if there has been a compromise, whichever is sooner. The Computing Coordinator and IT Support will be responsible for ensuring that passwords are changed.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out,

and will report to the Headteacher if there are any concerns. All USB peripherals such as key drives are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing the Staff Induction form to state they have read and understood the eSafety policy and the use of social media policy; students upon signing and returning their acceptance of the Acceptable Use Policy (parent's signature is also required).

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only, except in exceptional circumstances. The use of personal email addresses for work purposes is not permitted.

Where the curriculum calls for it, students are permitted to use the school email system, and as such will be given their own email address. The email address will be made up of their first name and a two-figured number, e.g. john09@Sherrier.leics.sch.uk. The use of individual emails begins in KS2 and therefore no KS1 children will have individual email addresses.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; Sherrier School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Sherrier School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school.
- Twitter – used by the school as a broadcast service (see below).
- Facebook – used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- The e-safety officer, Head, Deputy Head and School secretary have permission to post to the School Twitter Account.
- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using names.

- Where services are “comment enabled”, comments are to be set to “moderated”. When necessary, moderators have the responsibility of ‘turning off’ comments on a post if they are not appropriate.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner’s permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Dealing with offensive or derogatory comments - any inappropriate comments or activity by parents or other persons will be dealt with in the same manner as if it was face-to-face. Any inappropriate activity by members of school staff will be dealt with in accordance with the school policy.

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incident - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer and the Headteacher. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Sherrier School will have an annual programme of training which is suitable to the audience.

e-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student’s learning. Sherrier school employs the use of the Project EVOLVE Scheme. Within this scheme e-safety is teaching. Where the scheme is not used, staff are encouraged to note in their own plans any e-Safety issues that could arise. In addition, Sherrier School participates in Safer Internet Day every year.

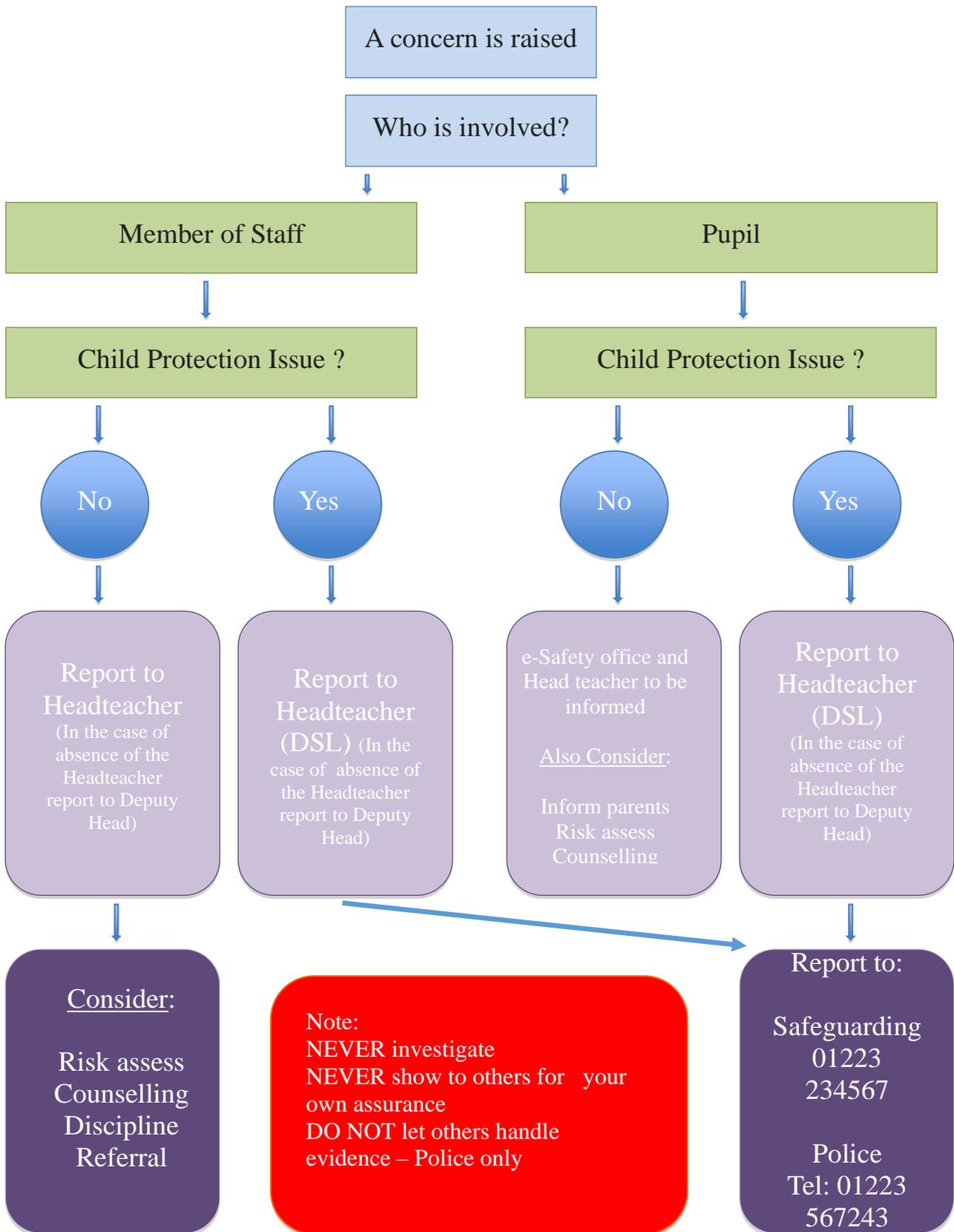
As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Appendix A- e-Safety Incident Log

Number:	Reported By: <i>(name of staff member)</i>	Reported To: <i>(e.g. Head, e-Safety Officer)</i>	
	When:	When:	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		Date:	
Signature (Governor)		Date:	

Appendix B- Inappropriate Activity Flowchart



If you are in any doubt, consult the Headteacher, Child Protection Officer or Safeguarding