CHANTLERS PRIMARY SCHOOL
E-Safety Policy

Approved by:	Governing Body	**Date:** September 2024
Last reviewed on:	September 2024	
Next review due by:	September 2025	

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 legal responsibility for the child/young person outside the school e.g. parent, guardian, or carer.

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

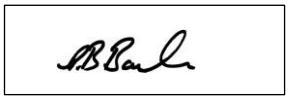
Wider school community – students, all staff, the governing body, parents and volunteers.

Safeguarding is a serious matter; at Chantlers 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 is twofold:

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

This policy is available for anybody to read on the Chantlers Primary School website; upon review, all members of staff will have read and understood both the e-safety policy and signed the Staff Acceptable Use Policy. The Students Acceptable Use Policy will be sent home with students on entry, at the beginning of each key stage and at the start of Year 5. Upon return of the signed reply slip, students will be permitted access to school technology including the Internet.

Headteacher Name: Mr P Barlow Signed: 

Chair of Governors: Signed:

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, ensures e-safety incidents were appropriately dealt with and ensures the policy was effective in managing those incidents.

- Appoint one 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 regarding training, identified risks and any incidents.
- Meet regularly with the ICT Manager and/or the ICT Class Coordinator.

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 ICT Manager who will work in consultation with the ICT coordinator, 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, the senior leadership team and governing body, and parents.
- The designated ICT Manager(s) has had appropriate CPD to undertake the day-to-day duties.
- All e-safety incidents are dealt with promptly and appropriately.

ICT Manager

The ICT Manager will:

- Keep up to date with the latest risks to children whilst using technology; familiarize yourself 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, the 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; 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 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.

Chantlers/Technical Support Staff

(Note: if you outsource (buy-in) your technical support this policy must be brought to their attention and signed as if they are a member of staff)

Technical support staff are responsible for ensuring that:

- The 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 systems) updates are regularly monitored and devices are 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; those categories of use are discussed and agreed upon with the ICT Manager and Headteacher.
- Passwords are applied correctly to all users regardless of age. Passwords for staff will be of high strength including upper & lower case letters, numbers and symbols.
- The IT System Administrator password is to be changed on a monthly (30-day) 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 ICT Manager (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 ICT Manager or the Headteacher to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.
- All must understand that they must not share personal passwords under any circumstances.
- Computers must be locked or logged off by the user when leaving unattended.

All Pupils

The boundaries of the 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 following the behaviour policy.

E-safety is embedded in our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware of 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 parent's evenings, school newsletters or workshops 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 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.

Named E-Safety Governor

The named Governor for e-Safety is responsible:

- To keep up to date with current advice on e-safety
- To advise on changes to the e-safety policy.
- To meet regularly (termly) with the Chantlers/Coordinator.
- To monitor the effectiveness (or not) of e-safety training and awareness in the school.
- To recommend further initiatives for e-safety training and awareness at the school.

Technology

Chantlers Primary School uses a range of devices including PCs, laptops, iPads and tablets. To safeguard the student and prevent the loss of personal data we employ the following assistive technology:

Internet Filtering – we use Sophos 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 response to an incident, whichever is sooner. The ICT Coordinator, ICT Manager and IT Manager 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 Sophos software that prevents any infected email from being 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.

Encryption – All school devices that hold personally identifiable data (as defined by the Data Protection Act 1998) are encrypted. No personally identifiable data is to leave the school on an unencrypted device; all devices that are kept on school property and which may contain personal data are encrypted.
NOTE: tablets and iPads are not encrypted so personally identifiable data must never be stored on them.

Any breach (i.e. loss/theft of devices such as laptops or USB key drives) is to be brought to the attention of the Senior Leadership Team immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner'sOffice.
(Note: Encryption does <u>not</u> mean password protected.)

Passwords – all staff and students will be unable to access any PC without a username and password. Some other devices such as the iPads and Galaxy tablets are not password protected. Staff passwords will change if there has been a compromise. Whoever discovers the compromise 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.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

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. Emails of a personal nature are not permitted. Similarly, the use of personal email addresses for work purposes is not permitted.
At present students do not have their school email addresses.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy and are re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year on entry, at the start of each key stage and at the start of Year 5; non-return of the permission slip will be assumed as acceptance.

Social Networking – there are many social networking services available; Chantlers Primary 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 Chantlers Primary School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the ICT Manager

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 and outside of school.
- Twitter – is used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method to share school information with the wider school community. No person will be "followed" on this service and as such no two-way communication will take place.

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

- 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 the first name and surname; the first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- 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 license that allows for such use (i.e. Creative Commons).

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

Incidents - Any e-safety incident is to be brought to the immediate attention of the ICT Manager or in his/her absence the Headteacher. The ICT Manager will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - The wider school community must be 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, Chantlers Primary School will have an annual programme of training which is suitable for 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.

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

The ICT Manager 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.

Acceptable Use Agreement – Staff

Note: All online and email activity is subject to monitoring

You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both you must sign this policy sheet.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; or any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the ICT Manager and an incident sheet completed.

Social networking – is allowed in school following the e-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with pupils on personal social networks

Use of Email – staff are not permitted to use school email addresses for personal business. All emails should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff student, or IT support.

Data Protection – If you must take work at home, or off-site, you should ensure that your device (laptop, USB pen drive etc) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given by the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the ICT Manager.

Viruses and other malware - any virus outbreaks are to be reported to the LGFL helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

E-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

NAME :

SIGNATURE: **DATE :**

Acceptable Use Statement – Students

Our Charter of Good Online Behaviour

Note: All online and email activity is subject to monitoring

I promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I know that I can be online when I am using a computer, laptop, phone, tablet or game console

I will – let my teacher know if anybody asks me for personal information online or on social media.

I will – let my teacher or parent/carer know if anybody says or does anything to me that is hurtful or upsets me online or on social media

I will – be respectful to everybody online and on social media; I will treat everybody the way that I want to be treated online.

I understand – that some people who are online or on social media are not who they say they are, and some people can be nasty. I will tell my teacher or parent/carer if I am ever concerned when I am online.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent): **Signed (Student):**

Class: **Date:**

Why do we, Filter and Monitor?

At Chantlers Primary School, we filter Internet activity for two reasons:

We filter to ensure

- (as much as possible) that children and young people (and to some extent adults) are not exposed to illegal or inappropriate websites. These sites are (or should be) restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
- (as much as possible) that the school has mitigated any risk to the children and young people, and thereby reduces any liability to the school by making reasonable endeavours to ensure the safety of those children and young people.

We monitor for assurance

- (as much as possible) that no inappropriate or illegal activity has taken place.
- To add to any evidential trail for disciplinary action if necessary.

A right to privacy?

Everybody has a right to privacy, whether adult or child. But in certain circumstances, there is a reduced expectation of privacy. In the context of this policy, that reduction is for security and safeguarding. This expectation is applicable whether it is school-owned equipment, or personally owned equipment used on the school network (and in some cases even if that personally owned equipment isn't used on the school network, but is used in school or for school business).

Managing Expectations

It is the expectations of the particularly important user; this will include school staff, students and parents/guardians of the students. Consent is not a requirement, however, we are required by law (Data Protection Act 1998) to make all reasonable efforts to inform users that we are monitoring them. By making reasonable efforts we are working "with" the students and parents, not just merely telling them.

Explaining to parents, staff and students

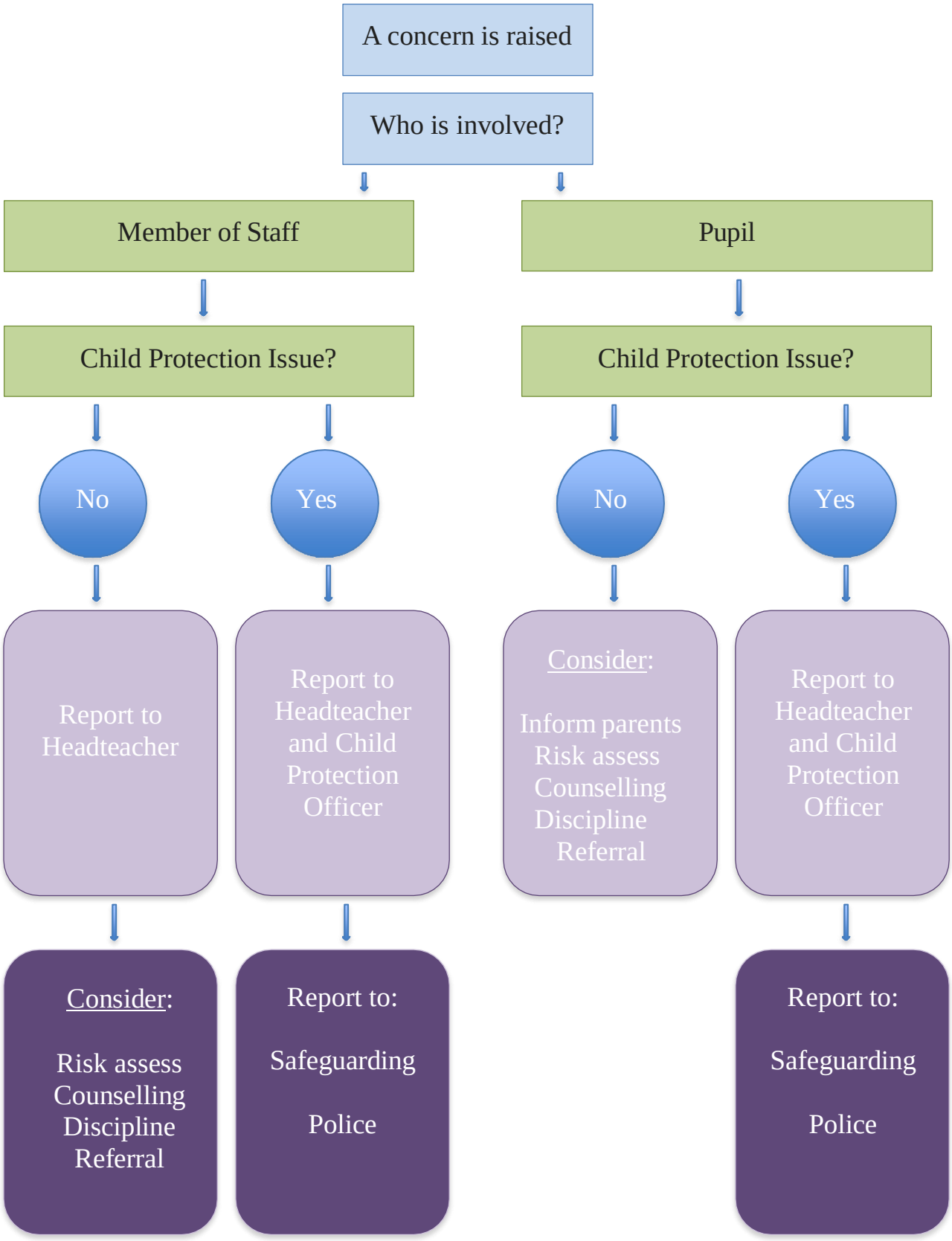
- Statement in Acceptable Use Policy, e.g. "Users are reminded that Internet activity may be monitored".
- Explain to staff why monitoring is important, allow them to voice any concerns and set their expectations of how the data can be used.
- Explain to the students as well, and allow them to ask questions.

E-Safety Incident Log

	Reported By: *(name of a staff member)*	**Reported To:** *(e.g. Head, ICT Manager)*
	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:**	

Inappropriate Activity Flowchart



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

Illegal Activity Flowchart