Chalton Lower School

E Safety (Acceptable Use) Policy

Document Control		
Edition	**Issued**	**Changes from previous**
1	01/11/23	Policy rewritten.

Policies/Documents referred to in this policy	Postholders/Persons named in this policy
Safeguarding/Child Protection Policy	Senior Information Risk Officer (SIRO) Headteacher Safeguarding Lead Computing Lead

Author: N Bill & F Mudd
Approved By: Governing Body

Issue Date: November 2023 To be reviewed: November 2026

Introduction

New technologies have become integral to the lives of children in today's society both within school and in their lives outside of school. It is both our responsibility and the right of all users,

that they can access the rich resource that is the World Wide Web and able to do so in a safe and secure environment. It is also the duty of the school to teach the children the necessary skills that enable them to make the right choices and remain safe, both inside and outside of the school environment. This framework of e-safety or acceptable use policy is to promote safe and appropriate use. As such, it should be understood in the context of other 'child protection' and 'behaviour' policies that the school already has in place. At Chalton Lower School the headteacher is the Senior Information Risk Officer (SIRO.)

The intention of the policy is:

- To maximize e-safety for all members of the school community.
- To help everyone understand the potential risks.
- To provide guidelines (including how the policy will be regulated and any sanctions) for safe and appropriate school and home use.

As such, the school more specifically intends:

- To provide a secure network for the school and secure means of home/school access.
- To log incidents and act accordingly.
- To establish key standards and behaviour for e-safety across the school, in-keeping with those of the local authority.
- To coordinate the activities for the school related to promoting best practice in e-safety, including the publications of guidelines and acceptable use policies for pupils, staff and parents.
- To ensure that we adhere to e-safety issues related to new government policies affecting schools.
- To monitor the schools responses to e-safety matters and act accordingly.

E-safety is a whole school issue and everyone in the school has a responsibility to promote it.

Guidelines

This policy aims to:

- Reflect the understanding that all members of the school community have responsibilities towards themselves, towards others and towards the school and that these responsibilities are not confined to the physical location of the school.
- Enable young people to develop their own protection strategies when adult supervision and technological protection are not available.
- Provide information on where to seek help and how to report incidents.
- Help young people understand that they are not accountable for the actions that others may force upon them, but that there are sanctions that the school will impose if they act inappropriately when online.
- Provide guidelines for parents, carers and others on safe practice.
- Ensure that the practice that it promotes is regularly monitored and reviewed with stakeholders.
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance and an effective e-safety programme. In school we are supported in doing this by Partnership Education our ICT support provider.

Strategy

Parents will be given advice about promoting e-safety both in school and at home. All pupils and parents are expected to sign an agreement to ensure safe use of the internet in school. E-safety guidelines and posters are displayed around the school.

Passwords

Staff passwords are kept private and only the password holder can change them. Access to Google Email, the Google Drive and Purple Mash is password protected and staff/pupils are advised not to share their password. It is accepted that from time to time, e.g. if forgetting a password, Partnership Education or the office manager can help pupils to obtain a new password. Staff laptops/computers must not be left in 'logged on' mode. (Ctrl + alt + delete, then lock) It is good practice for staff users to change their password regularly.

Emails

It is accepted that staff may send emails and attachments to recipients outside of the school using their school email address. School email addresses must only be used for school purposes. Pupils may only use their Purple Mash e-mail account. Pupils must immediately notify a member of staff if they receive offensive e-mail. Pupils must not reveal personal details of themselves or others in e-mail communication. If whole class or group e-mail addresses are used in school, this will be monitored by the class teacher. If required staff must only contact the pupils via their Purple Mash email and not through personal or other school emails.

Published Content and the School Website

The contact details on the school website should only be the school address, e-mail and telephone number. Staff or pupils personal information will not be published. The headteacher/office manager will take overall editorial responsibility of this to ensure that content is regularly updated and is accurate and appropriate.

Anti-Virus and Anti-Spam System

Chalton Lower School will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible. We will ensure that the policies and procedures approved within this policy are implemented. School ICT systems will be managed in ways that ensure that the school meets the e safety technical requirements outlined in the local authority e-safety guidance. The school has an up to date anti-virus and anti-spam system which is installed and provided by Partnership Education. Accessing the internet through the network will automatically ensure anti-virus protection and appropriate filtering is in place.

Video/Online Conferencing

Under the direct supervision of a teacher pupils may participate in online video-conferencing with other schools or organisations for the purposes of learning activities. This will usually be through the use of Zoom or Teams.

Access to Information

Information held by the school is defined and classified:

Restricted (named staff only)	Protected (all in school community)	Public (anyone)
Any info that identifies an individual	Routines, management info	School website, school Facebook page, ParentMail, displays

Access to all ICT systems shall be via a unique login and password. Any exceptions must be approved by the headteacher or computing lead. All information storage shall be restricted to

necessary users with any additional access being approved. The office manager must maintain a record of who has access to 'restricted' information.

Staff

The school aims to establish a clear understanding of the responsibilities of all those involved in the education of pupils and young people with regard to e-safety during staff training and safeguarding sessions. It is expected that all staff will read (and if necessary seek clarification) all school policies, including this acceptable use policy.

As such:

- Staff must not allow any emails between themselves and pupils to be anything other than school business.
- Staff must not have any pupil (or former pupils) as on-line friends if they are of school age.
- Staff must report to the computing lead any contact from a pupil or former pupil of school age.
- During ICT lessons pupils should be made aware of the procedures for reporting accidental access to inappropriate materials.
- Personal phones cannot be used during lessons or formal school time. However, staff may use their own phone during break times when they are not with the children, before and after the pupils arrive at school or to contact the school when off-site with the pupils i.e. when on a class trip.
  School email accounts should not be used for personal use.
- Staff should not conduct any personal transactions on school laptops as this could result in residual information remaining on the hard drive which may be accessible to others. The school cannot accept liability for any resulting loss or damage.
- Staff should keep to a minimum any data which is held on their school laptop and they must lock it if it is left unattended (ctrl +alt + delete, lock). The security of school laptops out of school lies with the staff who, by taking them off the school premises, accept responsibility for them.
- Guidance to staff, in respect of the appropriate taking of images is provided in the staff code of conduct. It is not appropriate for staff members to use personal digital cameras or camera phones on trips. A school camera/IPad or the school phone should be used for this purpose. Images should be transferred onto the school system.
- Parental permission for use of photographs is sought when the pupil starts school. Within one year of the pupil leaving the school, all photographs held electronically will be deleted.
- Any restricted data that is taken away from the school premises must be securely encrypted and only accessed on school devices.
- Exploring pupil data must only be on school devices.

Pupils

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.
- The school internet access will be designed for pupil use and will include filtering appropriate to the age of the pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. E-safety is an important element of this.

- The school cannot accept any responsibility for personally owned devices (e.g. laptops, USB devices, external hard drives, mobile phones and digital cameras) brought into school or taken on educational visits. They can only be taken on educational visits at the discretion of the teacher in charge and provided that pupils agree to use them appropriately as they would in school.
- The school accepts the use of school email addresses by pupils to communicate with other pupil and staff providing that these are via Purple Mash and during lesson time.
- Pupils learn about the good practice that is appropriate for social networking during ICT lessons.
- Pupils are made aware of the procedures for reporting accidental access to inappropriate materials.
- If pupils accidentally find inappropriate material they are to report it to an adult who will alert the headteacher and computing lead so that they can take steps to rectify this. Staff who find inappropriate material will report it directly to the computing lead, headteacher and Partnership Education. Staff are made aware of their responsibilities regarding this during staff training and by reading the policy.
- 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. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling E-Safety Complaints

Complaints of internet misuse will be dealt with by the headteacher and computing lead. Any complaint about potential or actual staff misuse must be referred to the headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.

Introducing the E-Safety Policy to Pupils

E-safety rules will be posted in the ICT suite and discussed with the pupils at the start of each year and discussed during future lessons. All pupils and their parent will sign an e-safety agreement form. Children are advised not to give out their own name or personal details over the internet without their parents' permission. It is expected that children in our school will have all of their internet access monitored at home. Pupils will be informed that network and internet use can be monitored.

Staff and the E-Safety Policy

All staff will be given the school e-safety policy and its importance explained. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting Parents Support

Parent's attention will be drawn to the school e-safety policy in newsletters, on the school web site and Facebook page. At the beginning of each curriculum year a letter advising parents of good practice at home regarding passwords, anti-virus and on-line safety is sent home together with a pupil and parent e-safety consent form.

Monitoring and Review

The computing lead is responsible for monitoring the standards of pupil's work and the quality of teaching in computing. The computing lead will support colleagues in the teaching of e safety by giving them information about current developments on the subject and by providing a strategic lead and direction. This policy will be reviewed regularly and any changes made will be clearly communicated to staff.

Appendix 1

Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. All staff must act in a trustworthy and responsible manner at all times and respect school

equipment. Members of staff should consult the school's e safety/acceptable use policy for further information and clarification.

- I will only use the schools e-mail, internet, Purple Mash, Google Drive and any related technologies for professional purposes.
- Images of pupils will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer. Images will not be distributed outside the school network without the permission of the parent/carer. Photographs and videos should only be taken using school equipment. Parents are asked to complete a
  "Photo Permissions Form for Pupils" on child's initial entry to the school.
- I understand that my use of school information systems, internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Senior Information Risk Owner (SIRO), the Designated Child Protection Coordinator and headteacher.
- I will ensure that electronic communications with pupils including email, Purple Mash and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with the students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- The school may exercise its right to monitor the use of the school's information systems and internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: ..... Capitals: ..... Date:.....

Appendix 2

Pupil Acceptable Use Agreement/E-Safety Rules

All pupils use computer facilities, including Internet access, as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign agreements to show that the e-safety Rules have been understood and agreed.

- I will only use ICT in school for school purposes.
- I will only e-mail people I know or who my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will act responsibly by telling a teacher or another adult.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video or give any other personal information that could be used to identify me, my family, my school or my friends unless my teacher has given permission.
- I will not arrange to meet someone I have only previously met on the internet or by email or in a chat room unless my parent or teacher has given me permission and I take a responsible adult with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I understand that my parent/carer will be contacted if a member of school staff is concerned about my e-Safety.

E-Safety Agreement

Name of Child

……..……Class……

Appendix 3

E-Safety Parental Consent Form

Parent/Carer Consent Form and E-Safety Rules

Parent/Carer Name: ……

Pupil Name: ……..…….

As the parent/carer of the above pupil, I have read and understood the attached school E-safety rules and grant permission for my daughter or son to have access to use the internet, school email system, Purple Mash and other ICT facilities at school.

My child has signed an E-safety agreement form. We have discussed this document and my child agrees to follow the E-safety rules and to support the safe and responsible use of ICT at Chalton Lower School.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching E-safety skills to pupils.

I understand that the school can check my child's computer files and that if they have concerns about their E-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's E-safety.

Parent/Carer Signature: ……..

Date: ……

Please complete, sign and return to your child's class teacher.

Appendix 4

Home and Family Guidelines

Being safe online is an important part of our Computing Curriculum. We ask parents to sign our e-safety agreement at the beginning of each year. Here are some of the guidelines we have for families about staying safe online.

☺ Talk together and have fun learning together.

☺ Keep virus and firewall software up to-date.

☺ Remember that passwords should be kept private and not shared with others. Many E-Safety incidents relate back to the sharing of passwords

☺ Involve everyone and agree your family guidelines and rules. Remember that sometimes what is acceptable for a 10 year old child is not necessarily acceptable for a 6 year old child.

☺ Regularly discuss online safety and go online with your children. **Communication** is the key to 'staying safe' online.

☺ Enable your 'browser safe' search option and/ or consider using internet filtering software and child-friendly search engines. Critically view all content as some websites are not what they appear.

☺ Keep the computer in a communal area of the house, where it's easier to monitor what your children are viewing. Do not let children have webcams, or similar, in their bedroom. **Remember any image, sound or text can be copied and viewed by everyone.**

☺ Talk to your children about why they should not to give out their personal details. If they want to subscribe to any online service then make up a family email address to receive the mail.

☺ We all love to chat and children are no different. Encourage your children to use moderated chat rooms and never to meet up with an online 'friend' without first telling you.

☺ Time spent online should be monitored to help prevent obsessive use of the internet. Children need to follow a range of activities many of which will be offline.

☺ Encourage your children, and in fact all family members, to tell you if they feel uncomfortable, upset or threatened by anything they see online.

☺ Have proportionate responses if the family guidelines are not followed.

Computers, games consoles, mobile phones etc are the doorway to the online world. **Think before you post online.**

Appendix 5

Chalton Lower School Incident Log
This should be reported on once a year to the governing body.

Date of Incident	Description	Immediate Corrective Action	Further Action	Legal Implications	Date of closure