eSafeguarding Policy

January 2023

Review by September 2025

1. Introduction

The requirement to ensure that pupils, staff and, indeed, all others in the school community are able to use the internet and related communications technologies appropriately and safely is part of the wider duty of care to which all who work in schools are bound.

This framework of E-Safety, or Acceptable Use Policy (AUP), 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 as well as other existing policies in respect of its employees such as the Staff Code of Conduct. Given the new technologies now available to use for educational purposes and in everyday life, the intention of this policy is:

- To maximise 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 design part of the school internet access expressly for pupil use and to include filtering appropriate to the age of pupils.
- To teach pupils what internet use is acceptable and what is not and give them clear objectives for internet use.
- To monitor traffic, 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 co-ordinate the activities for the school related to promoting best practice in E-Safety, including the publication of guidelines and acceptable use policies for pupils, staff, parents, and governors.
- To ensure that we adhere to E-Safety issues related to new government policies affecting schools.
- To monitor the School's responses to E-Safety matters and act accordingly
- To have a named school contact, Senior Information Risk Officer (SIRO)/E-Safety Co-ordinator, to coordinate the development and implementation of E-Safety policies, with clear designated responsibilities, and liaise with the Local Authority in such matters.

E-Safety is a whole school issue, not something that is simply the responsibility of the SIRO/E-Safety Co-ordinator. As such, the whole school has a responsibility to promote it.

2. Roles and Responsibilities

Although overall responsibility for e-safeguarding rests with the Headteacher, all e-safeguarding procedures outlined in this document assume the designation of named staff to the roles detailed below. It is the responsibility of the Governing Body and Headteacher to take corrective and disciplinary measures as are necessary when a breach of the Code of Conduct occurs and to contact and cooperate with police and other law enforcement agencies where a breach constitutes

a criminal act.

Responsibilities of all School employees

All employees must adhere to these standards when working on school premises, using equipment and utilities provided by the school at home or other locations and in all electronic communications with colleagues or children.

Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as text messaging, emails, digital cameras, webcams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny. The school's computers must not be used for private use, such as social networking or bank transactions.

Senior Information Risk Owner (SIRO/E-Safety Co-ordinator)

- The SIRO should be a member of the senior leadership team and have the following responsibilities:
- They keep a record of all Information Asset Owners (IAOs) on an Information Asset Register, see below
- They act as an advocate for information risk management

The SIRO should never be the network manager; the network manager implements decisions made by the SIRO. At Roecroft, the network is managed by our IT Consultants.

Information Asset Owners (IAOs)

These are the people who compile specific information and their role is to be clear about:

- What information they hold, and for what purpose.
- Who has access to the data and why.
- How information is retained and disposed of.

The SIRO maintains an Information Asset Register in line with GDPR which details the school's assets (IT systems) and who has access to them and why. Retention and disposal is detailed on our Retention Schedule.

Network Manager

The network manager is responsible for the performance, security and error detection of the network. They also implement access controls; this is the responsibility of our IT Consultants, Partnership Education and RM.

3. Acceptable User Polices (AUP)

AUPs must be signed by pupils and their parent/carer, staff, volunteers and some visitors to the school that need to have access to the school's network. It is the responsibility of staff to ensure that their visitors abide by the AUP. These forms are included at Appendix A, B and C.

The AUPs aim 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 begin to develop their own protection strategies in regard to E-Safety.
- 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 of an effective E-Safety programme.

4. Strategy

Our E-Safety policy has been written by the school, shared with major stakeholders and then approved by governors.

The E-Safety policy and its implementation will be reviewed every two years.

All parents are informed through the Home School Agreement and the pupils' AUP which is signed by them and their children when they start the school and again when they move into key stage 2. ICT rules are displayed in the computer suite and near classroom computers. Parents will be given advice about promoting E-Safety both in school and at home through posts on social media, extracts in the newsletter and annual E-safety parent/carer workshops organised by the ICT Lead.

When new employees join TJLS, they are given an induction which includes signposting important policies and procedures, this includes ICT & E-Safety. They are each given a copy of the Staff Handbook which includes the Code of Conduct detailing the IT AUP. Staff are asked to sign both an Induction form confirming that they have read and understood all the policies detailed on the form and that they will abide by the code. When policies are revised, employees are informed by email that they should read them again. Staff are asked every year to confirm that they have read and understood the latest policies by completing an online form through Dojo.

Volunteers are asked to sign a Code of Conduct and AUP prior to working in the school.

5. Access/Computer logins

Password Policy

Employee passwords are kept private and only the holder can change them, although some of them can be reset by admin users both within the school (for some applications) and by the school's IT Consultants or other software providers.

It is good practice for users to change their password regularly. Passwords must:

- be more than 8 characters long
- contain upper- and lower-case letter
- contain a number
- contain a special character (*&^%$)
- will expire every 6 months

Computers must not be left unattended in 'logged on' mode. Employees should lock their screens when they leave their desk by pressing the Microsoft logo and the 'L' key at the same time. Staff iPads should all be password protected and locked when not in use.

Access to the network is restricted according to job role.

Pupils

Pupils' access to devices is generic. Access to the network and internet is restricted.

Visitors/Volunteers

Visitors and Volunteers may be given access to the school's computers only on a restricted basis. Student teachers are provided with the generic pupil's login.

Visitors and volunteers may be provided with a unique guest WiFi code for their personal devices which has its own VLAN and does not interfere with the school's network. These codes are time limited and the duration of the code can be set by the School Operations Manager.

All volunteers receive a handbook prior to working with the school and must sign a volunteer agreement to show they have read and understood the handbook and any policies mentioned in the agreement, including this policy. (Appendix C).

See also section 14.

6. Google Drive for Staff

Staff are issued with an Google account and school email when they join us, depending upon their job role. They must change the password when they first log in. The school email account should only be used for school communications. All communications should be appropriate and professional. Teaching staff's email addresses are available on the school website, allowing parents to contact teachers directly if needed; if any concerns over a parent's email communication to a teacher arise, this should be reported to their phase leader and SLT and the email forwarded.

Employees should use their Google Drive to upload any data that they might need to work on at home or share with others. This is a way to keep data secure without the risk of losing a USB stick or laptop or the risk of emails being sent to the wrong address.

If employees add their Google Drive account to a personal device, then the following should be noted and is agreed:

Employees are reminded that if they set up their personal device to access Google Drive, they are reminded that use of such devices is dependent on their agreement with the school's Data Protection policy. Anyone choosing to use their own personal device should note that Google Drive's security capabilities can take control of their device's built-in security, including the remote wipe functionality – the school would never deliberately do this without the owner's consent. However, in the event that the device was stolen, the school data should be wiped as soon as possible and not be delayed waiting for the owner's consent. Employees must advise the school immediately if their device has been lost or stolen.

Employees are reminded that whilst personal devices are being used to access school documents via Google Drive, they should be set up securely and the device locked when not in use. It is best practice to sign out of Google Drive when it is not needed.

The following waiver is in place at this school.

Purpose

The purpose of this waiver is to define remote wipe technology and to ensure that employees understand and agree to its use if a remote wipe is necessary. The overriding goal is to protect the integrity of the school's data. Therefore, all users employing a mobile device that is connected to the school's network and/or is capable of backing up, storing, or otherwise accessing data of any type, has agreed to this remote wipe waiver.

Applicability

This waiver only applies to employees and devices that have access to the school's resources.

Remote Wipe

By connecting to the school's resources, mobile devices gain the capability of being selectively wiped remotely by our IT Consultants.

When a remote wipe is initiated by the user or our IT Consultants, the user's mobile device will be wiped of all the school's data. This data is not recoverable on the device itself but can usually be restored by reconnecting Google Drive and Company Portal applications and services. The remote wipe would not alter or damage any other information on the device.

A remote wipe will only be initiated if it is deemed absolutely necessary. Examples of situations requiring remote wipe include, but are not limited to:

- Theft of the device
- Loss of the device
- Termination of employment in which the user has not already cleared school data by another method.

7. Computer devices – Staff use

USB Sticks and use of server

Employees should not use USB sticks and should avoid saving personal data to their laptops. Instead, work can be saved to their Google account. Staff that need to can log on to the school server from home using the VPN installed on their laptops and access all school documents rather than saving content directly to their laptop. This avoids loss of data and eliminating USB use will prevent computer viruses being brought into school

Laptops

Employees are provided with a laptop according to their job role. A Laptop Loan Agreement must be signed when the device is first handed over and must be signed upon its return. Employees should not keep any sensitive data or photographs on their laptop for any longer than needed. Photographs should be uploaded to the server as soon as possible and deleted from the device. The Laptop Loan Agreement details the terms under which the device is loaned.

Loaned devices

If a device is on a short-term temporary loan, then this must be recorded in one of the school's Loan Logs maintained by the School Operations Manager. Instances could be:

- Device removed for repair by Partnership
- Loan of laptop whilst owner's is being repaired
- Loan of laptop for cover in a classroom

Personal devices

Use of personal devices, such as mobile phones must be limited to out of working hours. They must not be used to take photographs of pupils in school. Personal devices should be kept in cupboards during lesson time for all classes.

8. Staff Use of Social Networking Sites

The school's IT systems are regulated to only allow for appropriate use. It is important to remember that the use of these sites (even personal use out of school hours) could have an impact on the school, staff or pupils. A situation could easily arise where information posted could damage the school's reputation and constitute libel or defamation.

Safeguarding

Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. Adults should ensure that all communications are transparent and open to scrutiny.

Safeguarding children is the responsibility of all school employees. The key principles are:

Staff must not communicate (including accepting pupils as 'friends' requests) with any current pupils of the school, or from any other educational establishment, on social networking sites such as Facebook. This is applicable even if a school employee has permission from a pupil's parent/guardian (this would not apply to school aged pupils that an individual employee is directly related to, e.g. their child, niece or nephew). Staff should not communicate with, including being 'friends' with, past pupils whilst they are below the age of nineteen.

Principles apply:

- Regardless of whether access occurs during or outside of contracted work hours.
- To all technology whether provided by the school or owned by the employee.

Responsibilities

Staff are reminded that:

- Everything posted online is public, even with the strictest privacy settings. Once something is online it can be copied and redistributed. Therefore, assume that everything that is written is permanent and can be shared.
- They should have the highest standards of personal conduct (inside and outside of school).
- Ensure that their behaviour (inside and outside of school) does not compromise their position within the school.
- Ensure that their judgement and integrity should not be able to be brought into question.
- Ensure that their relationship with members of the community, via social media, does not compromise their position within the school.

Any failure to abide by this policy may result in disciplinary action. Staff must alert the governors or Headteacher where a breach of these standards is suspected or known to have occurred.

Unacceptable use of social networking sites/applications

Through social networking sites/applications, staff must not:

- Disclose private and confidential information relating to pupils, parents or other school employees, their employment directly or the school. This also applies to any other educational establishment that the employee has worked within.
- Discuss or reveal any matters relating to the school, previous educational establishments, school employees, pupils or parents.
- Publish, share, distribute or comment on any material that may be deemed contrary to British Values*.
- Identify themselves as a representative of the school.
- Write abusive comments regarding current/previous school employees, pupils or parents/guardians.
- Harass or bully school employees, persons unrelated or related to the school through cyber bullying and social exclusion.
- View or update their personal site (on Facebook, Twitter etc.) during their normal working day (this excludes breaks) and must ensure that their social networking site/application is secure at all times from third parties.
- Access or share illegal material.
- Publish any content, which may be deemed as defamation or discrimination.
- Post any images of pupils from the school or any other previous education establishment where the employee has worked.
- Without permission, post any images of school employees on social networking sites from the school or any other previous education establishment where the employee has worked.

- Set up and/or use an alias social networking account to circumvent the policy.
- Breach any of the school's other policies and procedures such as the school's Code of Conduct, Equal Opportunities Policy.
- Use it as a forum for raising and escalating concerns regarding the school or the Local Authority (these concerns should be raised using the Whistle Blowing Policy).

This list is not exhaustive and should be read in conjunction with the AUP.

** British Values are defined as those set out in statutory guidance 'The Prevent Duty' June 2015 and the Government advice in 'Improving spiritual, moral, social and cultural development of pupils' November 2014 and within any update to either publication*

School's social media account

The school has a Facebook account for parents to follow. The purpose of this accounts is to show parents updates upon school life; posts may include photos from school trips, topic days, charity events and other school events.

These accounts can only be accessed by designated members of staff and content can only be uploaded by this person, who should not share the login details with others. Should teachers wish to publish content on the account, then the post should be emailed to the designated member of staff who will check it with the Headteacher. Any photos that are emailed alongside the post should be checked to ensure that all children have permission from their parents to appear on social media.

School staff should not comment on these social media posts and avoid interacting with parent's comments. This account will be heavily monitored and any inappropriate comments from parents or staff will be removed.

9. Anti-Virus and Anti-Spam Software

The school uses the inbuilt RM firewall. This is updated by RM monitoring software and any patches required by devices are pushed out and installed (this includes OS updates).

If staff or pupils discover an unsuitable site, it must be reported on the Incident Log via the SIRO.

All users of emails must be alert to any malicious emails. Emails can be fraudulent even if they appear to come from a genuine source. Unless you are completely sure of the email's origin:

- do not open attachments that you have not asked for,
- do not click on links that will take you out of the email and
- do not enter any personal information or passwords, as no genuine unsolicited email would ask for them.

Anti-virus may not protect your computer and your data against new viruses. Please report any suspicious emails to the School Operations Manager or to Partnership by raising a ticket.

10. Protection of Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018, the General Data Protection Regulation 2016 and UK General Data Protection Regulations 2021 as amended from time to time. These acts aim to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School is dedicated to ensuring that the security of all information it holds and implements the highest standards of information security in order to achieve this, by taking full account of the recommendations of our IT consultants and our DPO (Paula Creighton of SPT Compliance Ltd).

11. 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 or device. Neither the school nor Central Bedfordshire Council can accept liability for the material accessed or any consequences of internet access.

The school, it's IT Consultants and the school's internet provider monitor traffic and can trace it to the individual user.

12. Handling E-Safety Complaints

Incidents of internet misuse must be logged in an IT Incident Book with the SIRO. Any complaint about staff misuse must be referred to the Headteacher. Any incident with a pupil will be dealt with in accordance with the school's Behaviour policy.

Incidents and/or complaints of a child protection nature must be dealt with in accordance with the school's Safeguarding policy.

For any complaint regarding indecent images, the flow diagram at Appendix F should be followed.

13. Published Content and the School Website

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. Photos of children will only be published with the authorised consent of parents/carers. They are asked to complete a consent form when they first join the school, although this can be amended at any time by the parent/carer. Summaries of consents are kept in classrooms and by office staff.

14. Access to Information

Teachers have access to a range of shared drives. The settings are determined by the level of sensitivity so not all staff can access all folders. Staff must remember to log off after completing their work and must not let pupils have access to the computers until then.

Inappropriate Content and Language

- For example, material that can be construed as offensive on the grounds of gender, race, ethnicity, disability, sexuality, religion, age, size/stature, status, TU membership.

- No partiality towards or against any political grouping or individual.

- The type of language that is used in emails should be no different to that which is used in face to face situations.

All staff should be aware of these pointers to keep pupils safe, but also why pupils should have fair access to ICT and the internet.

- 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 a part of the statutory curriculum and a necessary tool for staff and pupils.

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of 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.

- Pupils are not encouraged to bring into school personally owned devices unless they have been so requested by their teacher. These devices must not be connected to the school's network or WiFi.

- The school cannot accept any responsibility for personally owned devices (e.g. mobile phones) brought into school by staff or taken on educational visits. Staff should never take photos on their personal mobile device unless it is on a school trip, when the photo will be downloaded immediately upon return to school and deleted from all personal devices.

- School data should not be stored on personal devices.

- 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 advise the SIRO/E-safety Co-ordinator so that she can take steps to investigate this. Staff who find inappropriate material will report it directly to the SIRO/E-safety Co-ordinator. These will be noted in the IT Incident book (located on the staff server).

15. Introducing the E-Safety Policy to Pupils

E-Safety rules are posted in the ICT suite and in each classroom. They are discussed with the pupils throughout the year and referred to in computing sessions. When pupils move into key stage 2, both the pupil and their parents/carers will sign a new E-Safety agreement form. Children in lower year groups are advised not to give out their own name or personal details over the internet without their parent's permission. It is expected that children of this age will have all their internet access monitored at home.

Pupils are informed that network and internet use can be monitored.

16. E-safety curriculum

Pupils will engage in e-safety lessons throughout the year taught through our PSHE scheme of learning from Twinkl. The Twinkl programme uses the government recommended e-safety framework, 'Education for a Connected World'. The framework enables the development of teaching and learning as well as guidance to support children and young people to live knowledgeably, responsibly and safely in a digital world.

.

Teaching and learning of e-safety using this framework will be monitored by the ICT Lead who will carry out pupil voice activities, planning reviews and monitoring of learning. The ICT Lead will also provide staff with training within staff meetings when needed, with expectations for the e-safety curriculum regularly recapped.