E-Safety Policy

Approved by:	LSB
Last reviewed on:	March 2026
Next review due:	March 2027

This policy has been developed to ensure that E-Safety contributes to the fulfilment of the school aims.

To give children in our care the time, space and opportunity to develop their 'life in all its fullness' (John 10:10)

1. Introduction

The E-Safety policy sets out the key principles expected of all members of the school community here at Thrybergh Fullerton C of E Primary Academy, with respect to the use of ICT based technologies.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school / academy 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 covered by this policy, which may take place outside of the school / academy, but is linked to membership of the school / academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Updates in line with latest guidance KCSIE 2025:

Our school's approach to online safety reflects the latest requirements set out in *Keeping Children Safe in Education (KCSIE) 2025*. We recognise online safety as a core safeguarding duty and ensure that pupils are protected from risks arising from harmful content, contact, conduct and commerce online, including the newly emphasised threats of misinformation, disinformation and conspiracy theories. Our digital systems are supported by robust filtering and monitoring arrangements, with annual reviews carried out in line with strengthened expectations. We also embed cyber-security standards and the Department for Education's guidance on the safe use of generative AI to promote a secure and resilient digital environment for pupils and staff. Staff are trained to understand and respond to the full range of online risks, and parents are encouraged to engage in open discussions about their child's online experiences to help keep them safe beyond the school environment. The following explains in more depth how this is achieved.

1.2. Aims and objectives

The aims of E-Safety are to:

- Safeguard and protect the children and staff at Thrybergh Fullerton.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and / or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.

- Have clear structures to deal with online abuse such as cyberbullying, which are cross referenced within other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.
- Acceptable use agreements discussed and signed by all pupils.

2. Teaching and Learning style

Pupil e-safety curriculum

School has a clear, progressive e-safety education programme as part of the ICT/Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK
- To develop a range of strategies to evaluate and verify information before accepting its accuracy;
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- To know how to narrow down or refine a search;
- To understand how search engines work and to understand that this affects the results they see at the top of the listings;
- To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- To understand why they must not post pictures or videos of others without their permission;
- To know not to download any files – such as music files - without permission;
- To have strategies for dealing with receipt of inappropriate materials;
- To understand why and how some people will 'groom' young people for sexual reasons;
- To understand the impact of cyberbullying, sexting and trolling and know how and where to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Plan Internet use lessons carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Ensure children catch up if they miss these lessons due to absence from school.
- Will remind students about their responsibilities through an end-user
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling.
- We have E safety leaders in school. The leaders run assemblies and sessions to inform children about making the right decisions.

Staff and governor training

School ensures:

- Staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.
- Makes regular training available to staff on e-safety issues and the school's e-safety education program.
- Provides all new staff as part of the induction process, with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

School ensures:

- Parents / carers read the Acceptable Use Agreement, to ensure that principles of e-safe behaviour are made clear.
- Information leaflets; in school newsletters; on the school web site;
- Demonstrations, practical sessions held at school, if matters arise;
- Suggestions for safe Internet use at home;
- Provision of information about national support sites for parents.

3. Expected Conduct and Incident management

In this school, all users:

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Staff

- Are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

4. Incident Management

In school:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues.
- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA.
- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.

We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

5. Handling complaints:

The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by tutor / Head of school – Hannah Lambert / E-Safety Coordinator – Steffanie Plummer / Executive Head teacher – Claire Garbutt.
- Report is logged on CPOMS.
- Informing parents or carers.
- Removal of the Internet or computer access for a short time.
- Referral to LA / Police.

Our Safe guarding officer – Gina Lowry and E-Safety Coordinator – M Laycock acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Executive Head – Amy Gurner.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures. All reports are logged on to CPOMS so we can keep an ongoing record.

6. Monitoring and reviewing

The e-safety policy is referenced from within other school policies: ICT and Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

School has an e-safety coordinator / Safe guarding officer who will be responsible for document ownership, review and updates.

The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school

7. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

Our school:

- Has the educational filtered secure broadband connectivity through the RGfL and Schools Connect and so connects to the 'private' National Education Network;
- Secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site.
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform.
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons.
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network.
- Uses security time-outs on Internet access where practicable / useful.
- Works in partnership with the RGfL and Schools Connect to ensure any concerns about the system are communicated so that systems remain robust and protect students.
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Requires staff to preview websites before use [where not previously viewed or cached]. Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required. Is vigilant when conducting 'raw' image search with pupils e.g. Google image search.
- Informs all users that Internet use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems directly to the [*system administrator / teacher / person responsible for URL filtering]*. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or RGfL / Schools Connect Helpdesk as necessary.
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme.
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management (user access, backup)

In school to ensure the network is used safely we;

- Use individual, audited log-ins for all users.
- Ensure the Systems Administrator / network manager is up-to-date with services and policies / requires the Technical Support Provider to be up-to-date with services and policies;
- Make sure storage of all data within the school will conform to the UK data protection requirements

- Ensure staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide use the same username and password for access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with an individual network log-in username. From Group 2 they are expected to use their personal username and password;
- Makes it clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended. We request that they DO switch the computers off at the end of the day.
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Has set-up the network so that users cannot download executable files / programmes.
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes.
- Scans all computer memory sticks and storage devices with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data that complies with external Audit's requirements.
- Uses our broadband network for our CCTV system and have had set-up by approved partners.
- All computer equipment is installed professionally and meets health and safety standards.
- Projectors are maintained so that the quality of presentation remains high.
- Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

- Thrybergh Fullerton make it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it.

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

E-mail

- We provide staff with an email account for their professional use, *RGFL Staffmail.*
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of RGfL/Schools Connect provided technologies to help protect users and systems in the school, including desktop anti-virus products, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

Pupils:

Where necessary we use a class email which uses all the safety rules in place.
Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

8. School website

The Head teacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. The school web site complies with the statutory DfE guidelines for publications.

The point of contact on the web site is the school address, telephone number and the school email enquiries@tfp.dsat.education. Home information or individual e-mail identities will not be published.

Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website. We do not use embedded geodata in respect of stored images.

9. Social networking

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the *school /academy* or local authority.

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

10. Equipment and Digital Content

Personal mobile phones and modern technologies

- Mobile phones brought into school are entirely at the staff member, parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Modern technology—including mobile phones and any smart devices capable of sending or receiving messages, notifications, or recording audio or video—is not permitted for use by pupils during the school day to ensure a safe, calm and distraction-free learning environment. Following updated DfE guidance, the school prohibits the use of mobile phones and similar smart technologies throughout lessons, transitions, breaktimes and lunchtime, supporting high standards of behaviour and safeguarding all pupils online and offline. The school teaches safe, responsible and respectful use of technology through its e-safety curriculum, and any device brought into school must remain switched off and stored according to school procedures. These expectations help protect pupils from online risks, promote positive digital citizenship and ensure that modern technologies do not interrupt learning or wellbeing.
- Student mobile phones which are brought into school must be turned off (not placed on silent) and taken to the office. They are kept in the school office until the end of the day. Staff may use their phones during school break times but not in front of children.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Head teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times and not in front of children. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

Digital images and video

In school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.
- 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, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

- Details of all school-owned hardware will be recorded on the inventory list.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.