Trinity Road
Primary School
RESPECT • ACHIEVE • BELONG

E-Safety Policy

Reviewed by:	Senior Leadership Team
Reviewed:	Spring 2020
Ratified by Governors:	Spring 2020
Next Review:	Spring 2022

ICT has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- Tablets
- e-mail
- Instant messaging often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer, tablet or MP3/4 player)
- Social networking sites
- Video broadcasting sites such as Youtube and Tiktok
- Chat Rooms- including APPs and online communications
- Gaming Sites- where children can communicate through chat rooms and headsets
- Music download sites- with unfiltered language
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for children, staff and parent/carers.

What are the e-Safety issues?

Although the use of ICT and the Internet provide ever-increasing opportunities for children to expand their knowledge and skills, it is also the case that the use of such technology may sometimes expose children to the risk of harm such as;

- Children accessing Internet sites which contain unsuitable material (including fake news and hoax sites) or themselves posting unsuitable material;
- Children cyberbullying others or being cyberbullied;
- Posting and/or sharing personal information;
- Encouraging or being encouraged to display violent or extremist behaviour;
- Being contacted or making contact with strangers who may groom them for CSE, radicalisation or extremism.
- Pop up adverts which present unrealistic body images or gambling sites

Roles and Responsibilities:

e-Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to a member of the senior leadership team as part of wider Safeguarding responsibilities.

Our school e-Safety Co-ordinator is Jess Menown and Link Governor is Lisa Hibbert

Our e-Safety Coordinator works with the school ICT leader and ICT technician and ensures they keep up to date with e-Safety issues and guidance through organisations such as; Becta and The Child Exploitation and Online Protection (CEOP). The school's e- Safety coordinator ensures the senior leadership and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e- Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so children feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network (See Appendix 1);
- Safe use of school network, equipment and data (See Acceptable Use Policy);
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of child information/photographs and use of website;
- e-Bullying / cyber bullying procedures
- Their role in providing e-Safety education for children;

Staff are reminded /updated about e-Safety matters at least once a year in staff training as well as when specifics incidents may arise or legislation requires a change in procedure.

Internet searches are filtered through the school broadband provider. However, if something inappropriate should pop up, children are taught that they must inform an adult immediately so that this can be reported.

At Trinity Road, e-safety is embedded in the curriculum to ensure that every child has been educated about safe and responsible use. Children need to know how to control and minimise online risks and how to report a problem. The school uses the Google Internet Legends as a programme of study to support the requirements of the National Curriculum.

We ensure that we engage with parent/carers over e-safety matters and that parent/carers have signed and returned an acceptable use policy, highlighting the way ICT is used at school.

Communications:

How will we communicate with children on e-Safety?

- e-safety is within the Digital Literacy strand of the Computing Curriculum to raise the awareness and importance of safe and responsible internet use.
- Teachers will discuss the responsible and safe use of Internet access prior to any use in class.
- e-Safety will be highlighted and promoted during school assemblies on safety.
- All classes will promote the Google Be Internet Legends Code Of Awesome e-Safety rules.
- The Internet Legend Code will be displayed in all classrooms.

Just2Easy

Just2Easy offers a safe way for children to use technology to communicate with others in the school community and use interactive learning, assigned by their teacher. E-safety lessons are completed within their digital literacy module and half-termly to remind children of their responsibility to behave appropriately; whilst also ensuring that all children know how and when to report anything that they are uncomfortable about.

J2E allows teacher access, so all communications between children can be read. This is in addition to an automatic filtering system that will block emails containing inappropriate words and uploaded work has to be monitored and approved by administrators. Children should be shown and encouraged to notify their teacher on anything they receive that they feel uncomfortable about. Sanctions will be given according to the school behaviour policy, and a child's account may be closed, if deemed necessary.

Parents will be made aware of J2E and encouraged to supervise their child's internet usage. Parents should make the school aware immediately of any concerns. Class teachers should regularly monitor any photos uploaded onto J2E and ensure children are not accessing the website excessively or late at night. Staff and children have a code of conduct they are expected to follow when using J2E (Appendix 2.)

Training

As well as regular staff training, parents will be invited into school to receive e-safety training for parents. These events will be run when available or in response to local issues arising.

How will we communicate with staff on e-Safety?

It is important that all staff feel confident to use new technologies in teaching. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies.

Staff must understand that the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration, premises, governors and helpers should be included in appropriate awareness raising and training. Induction of new staff should include a discussion of the school's e-Safety Policy.

- Staff are aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff are aware that class desktops and laptops will be regularly monitored for photographic and video content. These should be deleted when used or transferred onto the school's hard drive.
- Staff will complete and sign an acceptable use policy agreement every year.
- Staff are aware that no personal digital equipment should be used within the school setting.
- Staff are informed that sensitive information should only be emailed in a password-encrypted file.
- Staff know that files should be saved onto a password-encrypted USB.

How will we communicate with parents/carers on e-Safety?

Internet use in children's homes is increasing rapidly. Unless parent/carers are aware of the dangers, children may have unrestricted access to the Internet. The school may be able to help parent/carers plan appropriate supervised use of the Internet at home.

- Internet issues will be handled sensitively, and parents/carers will be advised accordingly.
- A partnership approach with parents/carers will be encouraged. This may include parent/carer workshops with demonstrations and suggestions for safe home Internet use.
- Updates on the school's weekly newsletter or in letters out to parents/carers following any school concern.
- A specific area on the school website for E-safety with associated key links and guidance for parents and children.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parent/carers.

How will complaints regarding e-Safety be handled?

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 or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

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

- interview/counselling by class teacher / Phase Leader / Pastoral Support Worker/ Senior Leader / Leadership Team;
- informing parent/carers;
- removal of Internet or computer access for a period,
- referral to LA / Police.

Any complaint about staff misuse is referred to the Headteacher immediately. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the school and LA Safeguarding procedures.

The school's broadband

Appendix 1

Staff Social Networking Guidance:

e-Safety and the use of the Internet and Social Networking sites is an issue of high importance at Trinity Road Primary School. Please read and use the following guidance to ensure your own and our children's safety.

- Think carefully about your profile on any social networking sites. These may be viewed by children, parents or prospective employers. Lock down all of your privacy settings, but be aware that certain aspects of social networking may still be visible. What image of you does your profile portray? Be aware people are curious and may search for you.
- Never share personal details on any social networking sites. On feeds such as Twitter, it is possible to choose a user name which does not expose your identify and can then be passed only to people that you know and trust.
- NEVER add children on any sites. The legal age limit for using most social networking sites is 13 and, as a professional body, we should not be seen to be encouraging or condoning the use of these.
- Think very carefully about who you do add. Should parents/carers have access to aspects of your personal life? What image will this portray?
- Think carefully about any comments you post on other people's 'walls' or comments/status updates on your own profile page. What do these tell people about you or your views?
- Do not post pictures of children at school on any social networking sites. We have an obligation to ensure the safety of children and this includes the use of pictures/videos. Pictures of adults should only be posted with prior permission/knowledge of the people contained within them.

At all times, consider the effect the use of such sites could have on your professional reputation. How does what you post, re-tweet or follow, affect other people's opinion of you as a professional?

For further information, go to http://www.childnet.com/resources/social-networking-a-guide-for-teachers-and- professionals

Appendix 2

Trinity Road Primary School
Staff code of conduct for instructional videos and communication on J2E

On Instructional videos, staff need to ensure:

- They wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be neutral (for example, in front of a door or plain wall).
- The video should be recorded, reviewed and checked for suitability prior to uploading to J2E.
- Language must be professional, respectful and appropriate, including any family members in the background.

In any communication staff need to ensure:

- Language must be professional, respectful and appropriate, including any family members in the background.
- Written communication is clear, age appropriate and does not use 'text speak'
- Work is set and marked in accordance with Headteachers direction

Key point: Staff must only use the J2E platform provided by Trinity Road Primary School to communicate with pupils

Trinity Road Primary School
Pupil code of conduct for using J2E

It is important for our school values of Respect, Achieve and Belong to happen both inside and outside school, including online.

On J2E I will:

- Use respectful language when talking to adults on J2E
- Remember that it is a school platform and type in the same way I would write in my school books.
- Ask for help if I need it (with school work, home or your feelings.)
- Read carefully any instructions or feedback on my work by my teacher or any other school adult.
- Try just as hard as you would in school!

This policy should be read in conjunction with:

- Safeguarding Policy
- Code of conduct policy
- Acceptable use policy