Trinity All Saints CE Primary School

E-Safety Policy

Update: **March 2024**

Review Date: **March 2026**

Approved: March 2024 Review Date: March 2025

Signed Headteacher: Signed Chair of Governors:

1. Writing and reviewing the E-Safety policy

The E-Safety policy is part of the School Development Plan and relates to other policies including those for Computing, bullying and for child protection.

- The E-Safety co-ordinator is Mr David Morris, with our representative from Governors being Mr Michael Gration.
- Our E-Safety policy has been agreed by staff and approved by the Governors.
- The E-Safety Policy and its implementation will be reviewed annually.

2.1 Information system security

- School IT systems capacity and security will be reviewed regularly and updated when appropriate.
- Virus protection will be updated regularly.
- Passwords are given to all staff and children, and are updated annually.
- All staff equipment is password protected.

2.2 Email (when applicable)

- Pupils may only use approved e-mail accounts on the system (if necessary).
- Pupils must immediately tell a teacher if they receive an offensive e-mail
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- The forwarding of chain letters is not permitted.

2.3 Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number.
- Staff or pupil's personal information will not be published.
- The Computing co-ordinator in conjunction with office staff will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.4 Publishing pupil's images and work

- Pupils' full names will not be used anywhere on the website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or any other social media network.
- Photographs and videos will be stored securely on the school network and will be removed at the end of the year.

2.5 Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised to never give out personal details of any kind which may identify them or their location. All staff have signed the 'Code of Conduct for ICT Policy – Acceptable Use' with regards to maintaining a professional online profile.

2.6 Managing filtering and monitoring

- Filtering by definition is to: block access to harmful sites and content.
- Monitoring by definition is to: identify when a user accesses or searches for certain types of harmful content on school devices (it doesn't stop someone accessing it). The school is then alerted to any concerning content which can then be intervened and respond.
- The school will work with the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety co-ordinator or school technician.
- Filtering and monitoring will be in line with our Prevent Duty.
- The IT co-ordinator in conjunction with the IT technician will ensure that regular checks (monthly) are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Weekly filtering reports from Schools Bradford will be sent to C.Taylor.

2.7 Managing emerging technologies

- Emerging technologies will be examined for educational benefit by the IT co-ordinator.

2.8 Protecting personal data

Personal data will be recorded, process, transferred and made available according to the Data Protection Act 1998.

3. Policy Decisions

3.1 Authorising Internet access

- All staff must read and sign the 'Code of Conduct for ICT Policy – Acceptable Use' before using any school IT resource.

3.2 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. Neither the school nor the LEA can accept liability for the material accessed, or any consequences of Internet access.

3.3 Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by the E-Safety co-ordinator or a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure when necessary.

4. Communications Policy

4.1 Introducing the E-Safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils.

- Pupils will be informed that network and Internet use will be monitored.
- E-Safety is taught in all year groups, with all children understanding what they should do if an E-Safety incident occurs, and sanctions.

4.2 Staff and the E-Safety policy

- All staff will be given the School E-Safety Policy and its importance explained.
- E-Safety taught to all staff annually, with all staff understanding what to do with regards to an E-Safety incident.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

4.3 Enlisting parents' support

Parents' attention will be drawn to the School e-safety Policy in newsletters, the school brochure and on the school Web site. E-Safety is taught to parents annually.