



Trumps Green Infant School

E-Safety Policy

Trumps Green Infant School is committed to safeguarding, child protection and promoting the welfare of children and young people. We expect all members of the school community including staff, parents, carers, volunteers and governors to demonstrably share this commitment.

Introduction

The E-safety Policy is part of the School Development Plan and has been written by the school, building on best practice and government guidance using the Surrey model policy. It has been agreed by senior management and approved by governors.

This policy should be seen in the context of our related policies on Computing, Acceptable Use Agreement, Behaviour, Staff Discipline, and our range of safeguarding and equality policies.

Roles

The school has nominated E-Safety Leaders being Leigh Peters and Janine Bond (Computing Leads and Leigh being Deputy Headteacher and DSL in addition) and a responsible member of the Governing Body (Maggie Appleyard). The committee encourages input from all members of the school community to further e-safety practices.

Learning and Teaching

Why Internet and digital communications are important:

- 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 .i.e. through the use of Espresso and teacher shared internet sites such as Primary Resources.
- The school Internet access is provided by Surrey County through the RM contract and includes 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 will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content:

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught what is and how to report unpleasant/unexpected Internet activity to an adult.
- Pupils will be taught safe practice e.g. not disclosing personal information.

Managing Internet Access

Information System Security:

- All Internet use by pupils will be supervised
- School ICT systems security will be reviewed regularly.
- Virus protection will be monitored and updated regularly.
- Security strategies will be discussed with the Local Authority.

E-mail Usage:

- Teaching staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive or unexpected e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Published Content and the School Web Site:

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff, governors or pupil's personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupil's Images and Work:

- Pupils' full names will not be used on the Web site, as appropriate, including in blogs, forums, press releases, news articles or wikis, particularly in association with photographs.
- Parents are asked to complete a blanket permission slip relating to use of photographs when their children start at TGIS.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Managing Filtering:

- The school will work in partnership with Surrey County Council to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing Videoconferencing:

- Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing Emerging Technologies:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff will use a school phone where contact with pupils/parents is required.

IPads

We believe that the use of Apple iPads in teaching and learning can move children towards their learning goals. iPads are provided to each teacher and 6 iPads are provided for the pupils per year group.

- All iPads remain the property of the school and are to only be used by class teachers, support staff and pupils. iPads must not be loaned to other adults or pupils without agreement from the Headteacher.
- All teacher iPad's storing pupil photographs or assessment data must be password protected and comply with the high standards of data protection.
- When left unattended, iPads must be locked in a secure place within a locked room. It is the responsibility of the class teacher to ensure all iPads are securely locked away.
- All apps must be approved by the Computing co-ordinator/head-teacher before being downloaded on the school iPads

Protecting Personal Data:

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

Policy Decisions

Authorising Internet Access:

- All staff must read and sign the Acceptable Use Policy before using any school ICT resource. These should be returned to the Headteacher and stored in file
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Throughout the school, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Any person not directly employed by the school will be asked to sign an Acceptable Use of school ICT resources before being allowed to access the Internet from the school site.

Assessing Risks:

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Handling E-safety Complaints:

- Complaints of Internet misuse will be dealt with by the Headteacher.
- 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.

Community Use of the Internet:

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Communications Policy

Introducing the E-safety Policy to Pupils:

- Appropriate elements of the E-safety policy will be shared with pupils.

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.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting Parents' Support:

- Parents' and carers attention will be drawn to the School E-safety Policy through the school web site and newsletters.
- Parents and carers will from time to time be provided with additional information on E-safety.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Monitoring, Evaluation and Review

E-Safety is monitored in line with the Strategic School Development Plan policy monitoring cycle. The Governing Body monitors E-Safety within the school to evaluate its implementation and effectiveness. This policy will be reviewed by the Governing Body every three years, or earlier if the need arises. This policy will be promoted and implemented throughout the school.

Equality Statement

In accordance with our Equality Policy we will promote equality across the full range of protected characteristics and ensure that all pupils have equal access to all opportunities offered by the school.

Policy Status	
Agreed by Staff	September 2022
Agreed by Governors	September 2022
Next Review Date	September 2023