The Forest Family

Online Safety Procedure and Guidance

This e-Safety Procedures/guidance is part of a group of ICT security and Child Protection guidance documents and JTMAT policies and as well as other relevant documents. Please read in conjunction with T*eaching and Learning, ICT security file and relevant documentation, (ICT security, acceptable use – staff and pupils), child protection and anti-bullying, DSE, Staff discipline and code of conduct, community acceptable use, publication scheme, freedom of information, data protection and critical incidents as well as relevant risk assessments*.

The school's e-Safety officers are the Designated, Deputy designated and designated Governor Child Protection Officers.

The purpose of this and relevant ICT and acceptable use policies are to protect the integrity of the system and all of its users. The Forest Family schools will endeavour to provide a safe and secure environment for its users. *However, we cannot guarantee complete safety from inappropriate material. The responsibility must lie with each individual to use ICT in a safe, sensible and responsible way.* All users who access school ICT systems / website / VLE will be expected to sign an Acceptable Use Procedures/guidance before being provided with access to school systems.

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to prepare the children for the world of work, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations; improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DCSF; access to learning wherever and whenever convenient.

How the Forest Family will ensure our Internet use is safe:

- The school Internet access will be designed expressly for pupil use 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.

- Internet access will be planned carefully to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will maintain a current record of all staff and pupils who are granted Internet access. All staff read and sign the 'Acceptable ICT Use Agreement' at the beginning of each academic year. Annually, parents are informed that pupils will be provided with supervised internet access and are asked to sign and return a consent form for pupil access. Any parents who do not provide permission are recorded and other opportunities are provided for these children. (Often parents are happy for pupils to have access as long as it meets the above requirements)
- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the headteacher / ICT coordinator who investigate.
- School will ensure that the use of internet derived materials by pupils and staff complies with copyright law. Pupils are taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully in the same way as any correspondence going out from the school.
- The forwarding of chain letters is not permitted.

Social Networking (please read in conjunction with staff code of conduct)

- We block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Curriculum lessons cover all aspects of staying safe online.
- Pupils are advised never to give out personal details of any kind which may identify them or their location Pupils are advised not to place personal photos on any social network space.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Parents are reminded that any photographs they take of events are for their own personal use and not to be used on social networks. (If permitted)

Filtering

The school will work in partnership with the Local Authority, The John Taylor Multi-Academy Trust and the Internet Service Provider to ensure filtering systems (Sophos) are as effective as possible.

Monitoring

The school is monitored by Securus. The school staff liaise with Securus to manage any captures. DSL/DDSL staff investigate the captures and take suitable action.

Video Calling

- Video calls are planned and organised by teaching staff and pupils never hold video calls independently.
- Video calls 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.

- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden and will be dealt with through our behaviour guidelines and behaviour principles statement if outside school.
- Any staff, parents, visitors entering the EYFS will need to hand their phones into the office to be locked away. If staff or visitors are in any other areas of school, they will store them in the class cupboard. Staff, visitors who will be working with EYFS children or in their 'unit' will also hand phones in. Phones will only be used in offices or the staff room.

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 or pupils personal information is not be published.
- Staff ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils are always of groups will be selected carefully.
- Pupils' names will not be used anywhere on the Web site or Blog in association with photographs.
- Annually, parents are informed that we take photographic evidence of school life which may be used on the website or Twitter. They are asked to sign and return a consent form for pupil access. Any parents who do not provide permission are recorded and these children are not photographed.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Trust.

Protecting Personal Data

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

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 the trust or Staffordshire Council can accept liability for the material accessed, or any consequences of Internet access.
- The school audits ICT use to establish if the e-safety procedures/guidance is adequate and that the implementation of the e safety procedures/guidance is appropriate.

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 or Chair of Governors. 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.

Communication of Procedures/guidance

Pupils

- Rules for Internet access will be posted by all computers / in all classrooms.
- Pupils will be informed verbally of the procedures/guidance and taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils are informed that Internet use is monitored.

Staff

- All staff will be given the school e-Safety procedures/guidance annually and its importance is explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff receive GDPR and Cuber-Bullying annually.
- Parents' attention will be drawn to the school e-safety procedures/guidance in newsletters, the school prospectus and on the school Web site.