

E- safety Policy for



Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms (MLE) and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Downloading from the internet
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

At Forest Academy Primary School we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Principal and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in our school is Mrs Wray. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety coordinator to keep abreast of current issues and guidance through organisations such as CEOP and 'Think U Know'. The e-Safety coordinator updates Senior Management Team and Governors. All Governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and reviewing the e-Safety policy

This policy (for staff, governors, visitors and pupils), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: ICT, Home-school agreements, Behaviour, Health and Safety, Child Protection, and PSHE

policies including Anti-bullying.

Our e-Safety policy has been agreed by the Senior Management Team and Staff. The e-Safety policy and its implementation are reviewed annually.

E-Safety skills development for staff

- All members of staff receive regular information and training on e-Safety issues through the coordinator at staff meetings.
- All members of staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- All new members of staff receive information on the school's Acceptable Use Agreement as part of their induction.
- All members of staff incorporate e-Safety activities and awareness at the start of every term.
 - **Community use of the Internet**
- External organisations using the school's ICT facilities must adhere to the e-Safety policy.

Teaching and Learning

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach
- e-Safety.
- Educating pupils on the dangers of technologies that may be encountered
- outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if
- these issues affect them. Pupils are also aware of where to seek advice or help if
- they experience problems when using the Internet and related technologies; i.e.
- parent/carer, teacher/trusted member of staff, or an organisation such as
- Childline/CEOP.
- The school Internet access will be designed expressly for pupil use and will
- include 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.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Sophos anti-Virus protection is updated regularly by ADEPT Education.
- System security is overseen by our technicians (Mircea Astefanoae)

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published content and the school web site

The contact details on the school website are the school address, e-mail and telephone number. Staff or pupils' personal information is not published. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the school website, particularly in association with photographs.
- Pupils' work can only be published by outside agencies with the permission of the pupil and parents.

Photographs taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites, e.g. School performances and assemblies etc.

Social networking and personal publishing

- The school blocks access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate and or illegal (e.g. Facebook) for primary aged pupils.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff are advised not to add children, or parents as 'friends' if they use these sites. Please refer to the School's Safeguarding policy and School's code of conduct.

Managing filtering

- Has the educational filtered secure broadband connectivity through the LGfLand so connects to the 'private' National Education Network.
- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
- All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status.
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students.
- Ensures network is healthy through use of Sophos anti-virus software (from LGfL) etc and network set-up so staff and pupils cannot download executable files
- Uses individual, audited log-ins for all users - the London USO system
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, 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
- Provides highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils; Uses London mail with students as this has email contencontrol and the address does not identify the student or school
- Provides staff with an email account for their professional use, London Staffmail

/ LA email and makes clear personal email should be through a separate

Account

- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students

- Ensures the Systems Administrator / network manager is up-to-date with LGfL

services and policies / requires the Technical Support Provider to be up-to-date

with LGfL services and policies

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.
- The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material.
- Pupils are only allowed to bring personal mobile devices/phones to school if they are in Year 5 or 6 and they are travelling home alone. Any phones that are brought to school are kept by the office until the end of the day.
- The sending of abusive or inappropriate text messages or emails outside school is forbidden.
- Staff will use a school phone where contact with pupils is required.

Breakfast and after school club have a mobile phone to contact parents and for parents to book sessions for their children.

Protecting personal data

The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school.

The school will hold personal information on its systems for as long as individual members of staff remain at the school and remove it in the event of staff leaving or until it is no longer required for the legitimate function of the school.

We will ensure that all personal information supplied is held securely, in accordance with the GDPR Data Protection Act 2019.

Each teacher has the right to view personal information that the school holds and to have any inaccuracies corrected.

Policy Decisions

Authorising Internet access

☑ Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement (AUA) for pupils and abide by the school's e-Safety guidelines.

☑ Access to the Internet will be by directly supervised and to specific, approved on-line materials.

☑ All staff using a school laptop will be made aware of the schools Laptop Use Policy

Password Security

☑ Adult users are provided with an individual network username and password, email address and Google Drive username and password, which they are encouraged to change periodically.

☑ Key Stage Two pupils are provided with an individual Google Drive username and password.

☑ All members of staff are aware of the dangers inherent in leaving the SIMs system, for pupil-tracking and digital registers, open and of the importance of keeping passwords secret

☑ All members of staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. The school will audit ICT provision to establish if the e-Safety policy is adequate and that its implementation is effective.

Handling e-Safety complaints

☑ Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the e-Safety coordinator.

☑ Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety coordinator

☑ Any complaint about staff misuse must be referred to the Headteacher.

☑ Complaints and concerns of a child protection nature must be dealt with in accordance with school child protection procedures. For example evidence of: inappropriate online relationships; a child watching pornography or any '18' films on a regular basis; online/digital bullying, harassment or inappropriate image sharing etc.

☑ Pupils and parents will be informed of the complaints procedure.

Communications Policy

Introducing the e-Safety policy to pupils

☑ E-Safety rules are displayed in the classrooms and discussed with the pupils at the start of each term. All staff are aware that at least one dedicated e-safety lesson must be taught each term and at relevant points throughout e.g. during PSHE lessons//anti-bullying week/Safer Internet Day.

☑ Pupils will be informed that network and Internet use will be monitored.

The school is vigilant when conducting 'raw' image search with pupils e.g.

Google or Lycos image search

☑ Pupils are required to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme

Staff and the e-Safety policy

☑ All staff must sign the Staff Acceptable Use Policy (AUP) and a copy is kept on file.

☑ Any information downloaded must be respectful of copyright, property rights and

privacy.

☒ All members of staff are aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

☒ A laptop issued to a member of staff remains the property of the school (see laptop use policy). Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

Parents and the e-safety policy

☒ All parents, when their child joins the school, will be asked to sign the AUA for pupils giving consent for their child to use the Internet in school by following the school's e-Safety guidelines and within the constraints detailed in the school's e-Safety policy.

☒ Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.

☒ Parents are encouraged to look at the school's e-safety policy and the two pupils' 'Acceptable User Agreements' (for KS1 & KS2)

☒ Parents receive an e-safety bulletin attached to the school newsletter at least once per term

The Learning Platform and other home/school internet use

☒ All staff have been trained and given advice on how to effectively use the Google Drive and SIMs

☒ Parents will be informed about what the Google Drive and other self-contained blogging platforms (LGfL) are and how it can enhance the learning of each child.

All children will be given training on how to effectively use Google Drive and other blogging platforms (LGfL)

☒ All children will be given a username and password to access secure resources and facilities on the Google Drive.

☒ The school website forums will be regularly monitored for incidents of cyberbullying, inappropriate use of language or the uploading of inappropriate files.

Children will be informed that the sending of messages is

monitored and misuse of the messaging system will result firstly in a warning,

followed by removal as a user from the service should such behaviour be repeated.

☒ Class teachers will monitor the use of the Google Drive and school website forums. Any misuse of the Google Drive/school website forums will be reported to the Headteacher.

Our safeguarding policy covers online meetings to protect our families and staff with the following guidance before a child's zoom meeting:

☒ All Zoom class meetings will be recorded by the school and kept for a month.

☒ Children must wear suitable clothing, as should everyone else in the household e.g. no nightwear or swimwear

☒ When staff are using platforms such as Zoom, meetings will always take place with a senior leader present.

☒ Every child accessing the Zoom meeting from home should have a parent or carer within ear shot for the duration of the conversation.

☒ Sessions will only take place with the authorisation of a member of the Senior Leadership Team.

☒ Any computers used should be in communal areas or rooms i.e. not in bedrooms; and the background should be blank or blurred, where possible.

☒ Zoom meetings should be kept to a reasonable length of time (30 minutes).

☒ Language must be professional and appropriate at all times.

☒ Staff must only use platforms provided by Forest Academy to communicate with pupils

☒ Children accessing the meeting from school will use an iPad in a classroom with their classmates and be supervised by a member of staff.

On-line learning will be delivered via the school website, under the Home Learning tab. Pupils who do not have access to the internet will be able to obtain hard copies from the school office.

Virtual assemblies may be accessed from home, also via the school website.

In the event of a lockdown, weekly phone contact will be made with each child and their family.

Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored on an annual basis by the e-Safety Coordinator (Mrs Wray).

This policy is the Governors' responsibility and they will review its effectiveness annually.

They will do this during reviews conducted between the e-Safety Coordinator and the Designated Child Protection Coordinator. Ongoing incidents will be reported to the full governing body.

Implemented October 2020

To be reviewed: October 2021.