E-safety Policy

Excellence for All

Policy reviewed/updated	September 2024
Next update	July, 2026
Committee	Pupils & Personnel Finance & General Purposes
Executive Headteacher	Mr Ben Waldram
Chair of Governors	Mr Pete Cumberland

Revision date	Author of changes	Summary of changes
12.9.24	J Hartley	Update to esafety provision (lessons); addition of filtering and monitoring service; update to virus protection system.

E-safety should be a focus in all relative areas of the curriculum and staff should re-enforce e-safety messages across the curriculum.

Introduction

At Fernwood Primary and Nursery School, we understand that e-safety encompasses an ever-widening range of Internet technologies and electronic communications across all areas of the curriculum. The E-safety policy highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online activities.

The school's E-Safety Policy should operate in conjunction with the school's other policies including those for Child Protection, Behaviour and Anti-Bullying, S.R.E, P.D. and Acceptable Usage Policy.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies
- Implementation of E-Safety Policy in both administration and curriculum, including secure school network design and use
- Safe and secure network including the effective management of filtering systems.

Roles and Responsibilities

Our E-Safety Policy has been written by the school. It has been agreed by the staff and governors. A member of the governing body has taken on the role of e-safety governor, they will work in collaboration with the Executive Headteacher, the Head of School, the Network Manager and Computing Subject Leaders. E-safety issues are included in the Child Protection, Health and Safety and Anti-Bullying policies, along with the Staff Code of Conduct.

The E-Safety Policy will be reviewed biannually.

Teaching and Learning

Pupils will be taught what Internet use is acceptable, what is not and given clear objectives for said Internet use. The school's Internet access will include appropriate filtering. Any Internet access will be planned to enrich and extend learning activities. A planned e-safety curriculum is delivered and regularly revisited through engaging computing lessons. In addition, key e-safety messages are re-enforced through assemblies and school newsletters.

Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in effective use of the Internet including research, retrieval and evaluation. Pupils should be taught to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy. They should also be aware and respect copyright laws when using materials accessed on the Internet.

If staff or pupils discover unsuitable sites, they must report this to a member of SLT.

We offer training and information for staff to support their understanding and teaching of E-safety. Children attend assemblies where focused e-safety teaching is delivered. A session is offered to parents to support their understanding of e-safety, links are provided on the school website regarding e-safety and an e-safety update is regularly published in the school's newsletter.

We continually look for new opportunities to promote E-safety:

- We provide opportunities within the Computing and Personal Development curriculum to teach about E-safety.
- Educating pupils about the dangers of technologies encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Pupils are taught about respecting other people's information, images etc through discussion, modelling and activities as part of the computing curriculum.
- Pupils are aware of the impact of online bullying through Personal Development lessons and are taught how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (cyberbullying).
- Pupils are taught to critically evaluate materials and learn good searching skills through the computing curriculum.
- Pupils are taught about the risks inherent in using social media, particularly if they are contacted by people they do not know.

E-Safety Curriculum

As from September 2024, we now have a stand-alone E-Safety curriculum that is delivered to all pupils across our school from Nursery to Y6. This curriculum has been based on the Evolve Website, which contains up-to-date information and is itself updated regularly to keep on top of an ever-changing digital landscape. This new curriculum will be updated yearly.

Managing Internet Access

The security of the school information systems is reviewed regularly. Virus protection is installed and updated often. The school uses a company called Wave9 for the onsite filtering and full reporting to comply with PREVENT, KCSIE (Keeping Children Safe In Edcuation) & CTIRU (Counter-Terrorism Internet Referral Unit) – Provided via a Sophos XG Firewall (Support by Wave 9). The system takes all reasonable precautions to ensure that users access only appropriate material. Due to the international scale and linked nature of Internet content, it is not possible to guarantee that inappropriate material will never appear on a school computer. All matters of concern should be reported to the Executive Headteacher or Head of School immediately.

Children are not allowed access to personal e-mail accounts or chat rooms whilst in school. Pupils should immediately tell a teacher if they receive any offensive communication. Pupils must not reveal any personal details of themselves or others online.

Any digital communication (websites, blogs, email or text) between staff and pupils/parents must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications. The contact details on the website should be the school's address, e-mail and telephone number. Staff or pupils' personal information will not be published.

Staff have received PREVENT training and are aware of the many dangers children can face online such as radicalisation and child sexual exploitation. If a member of staff is concerned that any child is at risk, they must follow safeguarding procedures.

Staff must preview any recommended sites before use. Particular care must be taken when using search engines with the children as these can return undesirable links. Raw image searches are discouraged when working with pupils. If internet research is set as homework, specific sites will be suggested, that have previously been checked by the teacher. It is advised that parents check these sites too and supervise work. We use a third-party piece of software called Fastvue - this software works alongside the Sophos XG firewall. FastVue. It will alert for areas such as: Extremist Websites, Self-Harm, Drug related, Adult and Profanity searches etc and lots more in real time. If Pupils or Staff do search for these areas, the software actively alerts our designated senior lead team about it, and lists the user and device IP address. These are then sent to a member of the SLT via automated email.

Personal Usage

Personal devices **must not** be used by staff or pupils within the school setting. Social networking sites and newsgroups will be blocked unless a specific use is approved. Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, phone numbers or e-mail address etc. Pupils' parents are advised that the use of social network spaces outside school are inappropriate for **all** primary aged pupils.

When using digital images or videos, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of these images or videos. In particular, they should recognise the risks attached to publishing their own content on the internet.

Emerging Technologies

The school is aware of emerging technologies and the benefits or dangers these could present to children. Emerging technologies will be examined for educational benefit and an assessment of risk carried out before use in school is allowed.

Children bringing mobile phones drop them off at the school office at the start of the day. The phones will have been brought by our older children who require a way to contact parents to enable them to get home safely. Smart watches are occasionally used across KS2, with the primary reasons being telling the time and counting steps. Although we encourage this technology as a health and well-being monitoring system, we do not allow smart watches which take photographs or have their own ability to communicate (text, calls, etc).

Policy Decisions

All staff must read and sign the Acceptable Usage Policy before using any school computing resource. Internet usage in school is supervised by a responsible adult and children are allowed access to approved online materials. Children are encouraged to be vigilant users and report inappropriate usage to an adult. The Executive Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy monitored.

Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Executive Headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Communicating

The school will respond to Internet-related issues experienced by pupils out of school, e.g. social networking sites, cyber-bullying and offer appropriate advice and or sanctions if required. Pupils will be informed that Internet use will be monitored in school. Advice on E-safety will be introduced at an age-appropriate level to raise the awareness and importance of safe responsible Internet use.

All staff will be given the School E-Safety Policy and its importance explained. Staff should be aware that Internet traffic is monitored and traced to the individual user. Discretion and professional conduct is essential.

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (2018).