Elmwood Infant and Nursery School

E-Safety Policy

Article 17 'Children have the right to get information that is important for their well-being, including from computers. Adults should make sure that the information they get is not harmful.'

Elmwood Infant School & Nursery

E-Safety Policy

Article 17 'Children have the right to get information that is important for their well-being, including from computers. Adults should make sure that the information they get is not harmful.'

Date Policy Agreed: Spring 2020
Review Date: Spring 2023

Introduction

At Elmwood Infant School we believe that Computing is central to all aspects of learning; for adults and children in both the school and the wider community. Provision should reflect the rapid developments in technology.

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to equip our young people with the skills to access lifelong learning and employment.

All children, whatever their needs, will have access to a range of up to date technologies in both the classrooms and everyday environment. ICT is a life skill and should not be taught in isolation.

Information and Communications Technology 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 are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blog
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming and apps
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

All users need to be aware of the range of risks associated with the use of these Internet technologies.

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

‘Schools are finding that a blocking and banning approach, which merely limits exposure to risk, may no longer be a sustainable approach… Schools need to focus on a model of empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks’

(Becta Safeguarding Children Online)

This e-safety policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communication as a whole.

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults and young people while on the school premises.

Related Documents:

- Acceptable Use of the Internet Policy
- Early Help and Safeguarding Policy
- GDPR Policy
- Behaviour Policy
- Anti-bullying Policy
- Computing Policy

Publicising e-Safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website.
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated
- Post relevant e-Safety information in all areas where computers are used
- Provide e-Safety information to parents via the website and when necessary through newsletters at the beginning of each term.

Whole School Approach

All members of the school community have a responsibility for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures. This includes vigilance when children are accessing the internet at school to ensure that they do not access inappropriate websites.

All staff should be familiar with the school’s policy including:

- safe use of e-mail
- safe use of the Internet
- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on the school website
- procedures in the event of misuse of technology by any member of the school community
- their role in providing e-safety education for pupils.

Staff are reminded/updated about e-safety regularly and new staff and students receive information on the school's acceptable use policy as part of their induction. Supply Teachers must sign an acceptable use of ICT agreement before using technology equipment in school

Roles and Responsibilities

The Head and Governors have ultimate responsibility for establishing safe practice and managing e-Safety issues at our school. The role of e-Safety co-ordinator has been allocated to the headteacher. They are the central point of contact for all e-Safety issues and will be responsible for day-to-day management.

All members of the school community have certain core responsibilities within and outside the school environment.

The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the Deputy Safeguarding Leads, the Safeguarding and E Safety governor and the governing body.
- Work with governors and staff to review and update online safety policies.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of Conduct /Acceptable Use Policy for staff and governors.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with the computing technician to monitor the safety and security of school systems and networks.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate online safety practice to identify strengths and areas for improvement.

It is the responsibility of all members of staff to:

- Contribute to the development of online safety procedures.
- Read and adhere to this E-safety Policy, the Safeguarding and Child Protection Policy, the ICT Code of Conduct /Acceptable Use Policy and the Staff Code of Conduct.
- Take responsibility for the security of school systems and the data they use or have access to.

- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education into the curriculum.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

It is the responsibility of the Headteacher to:

- When required, develop and implement appropriate online safety policies and procedures.
- Implement appropriate security measures to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Investigate any filtering breaches and ensure that any safeguarding concerns, identified through monitoring or filtering breaches are dealt with appropriately.
- Monitor the on-line activity of staff and pupils and deal with any issues as appropriate.
- Ensure that staff adhere to this this E-safety Policy, the Safeguarding and Child Protection Policy, the ICT Code of Conduct and the Staff Code of Conduct.

It is the responsibility the computing technician to:

- Provide technical support and perspective to the school, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures, including password policies and encryption, to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the school's filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

Pupils are taught to:

- Engage in age appropriate online safety education opportunities under the direct supervision of school staff.
- Understand child-friendly online safety procedures during curriculum and teaching time.
- Read and adhere to the school's pupil-friendly Acceptable Use posters that are displayed in the classrooms and the ICT suite.
- Understand how to seek help from a trusted adult if they experience an on-line concern.

It is the responsibility of governors to:

- Hold the school to account to ensure that robust safeguarding, E-safety and on-line procedures and policies are in place and are being adhered to.
- Undertake safeguarding and child protection training that includes on-line and E-safety training.
- Read and adhere to this policy and to the school's Acceptable Use Policy.

It is the responsibility of parents and carers to:

- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement statements that relate to the use of social media and other e-safety issues.
- Identify changes in behaviour that could indicate that their child is at risk of harm online. If appropriate parents should inform the school for extra support and advice.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Physical Environment / Security

The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the LA where appropriate.

- Anti-virus software is installed on all computers and updated regularly
- Central filtering is provided by AdEPT Education (LGfL) and managed by the school. All staff and students understand that if an inappropriate site is discovered it must be reported to the headteacher. All incidents will be recorded in the behaviour book.
- All staff are issued with their own username and password for network access. Trainee teachers and long term supply staff are issued with temporary IDs and the details recorded. Other students/ visitors will be issued with a temporary username/ password on request
- Foundation stage pupils use class name logon IDs for their network access
- Key stage one pupils logon with their own name.

Mobile / Emerging Technologies

- Teaching staff at the school are provided with a laptop for educational use and their own professional development. All staff understand that the Acceptable Use Policy applies to this equipment at all times.
- To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network.
- Staff understand that they should use their own mobile phones sensibly and in line with guidance in the Staff Handbook
- The Educations and Inspections Act 2006 grants the Head the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head will exercise this right at her discretion
- Pictures / videos of staff and pupils should not be taken on personal devices.
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community

E-safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety.

We provide opportunities within the Computing and PSHE curriculum areas to teach about e-safety by:

- Educating pupils on the dangers of technologies that may be 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 PSHE 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 about the risks inherent in using social media, particularly if they are contacted by people they do not know.

E-mail

The school e-mail system is provided and filtered by AdEPT Education (LGfL) and monitored by the computing technician. The use of email within school is an essential means of communication for staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school, between schools or international. We recognise that pupils need to understand how to style an email in relation to their age.

All staff are given a school e-mail address and understand that this must be used for all professional communication. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

- Key stage one pupils have access to class based e-mail accounts that can be monitored by the class teacher.
- Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication
- Staff are allowed to access personal e-mail accounts on the school system outside directed time and understand that any messages sent using the school equipment should be in line with the Acceptable Use policy. In addition, they also understand that these messages will be scanned by the monitoring software
- Everyone in the school community understands that any inappropriate e-mails must be reported to the class teacher / e-Safety co-ordinator as soon as possible
- Pupils are introduced to email as part of the Computing Scheme of Work.
- Under no circumstances should staff contact pupils or parents using personal email addresses.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail. All pupils must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone. Staff must inform the headteacher if they receive an offensive e-mail.

Published Content

The Head takes responsibility for content published to the school web site but delegates general editorial responsibility to Matt Devonshire. Staff are responsible for the editorial control of work provided for publication.

- The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution.
- The school encourages the use of e-mail to contact the school via the school office
- The school does not publish any contact details for the pupils

Digital Media

We respect the privacy of the school community and n a child's entry to the school, all parents/guardians will be asked to give permission for their child's photo to be taken and to use their child's work/photos before any images or video are published or distributed outside the school:

- Photographs published on the website will not identify any individual pupil by name
- Students' full names will not be published outside the school environment

Social Networking and Online Communication

The school currently allows limited access to social networking sites for example, You Tube and email for educational purposes but not for personal use. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Guidance is provided to the school community on how to use online communication safely and appropriately. This includes:

- Being selective about publishing personal information
- not publishing information relating to the school community
- how to report issues or inappropriate content

Unmoderated chat sites present an unacceptable level of risk and are blocked in school. Pupils are given age appropriate advice and guidance around the use of such sites as the need arises. Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Any external matters evolving from a social networking site will not be supported by the school.

Educational Use

School staff model appropriate use of school resources including the internet.

- All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material
- Where appropriate, links to specific web sites will be provided instead of open searching for information
- Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Polices before any activity

E-safety Training

The school has a program of continuing professional development in place that includes; Safeguarding INSET, in school support and E-safety assemblies based on the needs of the staff and children.

- Educational resources are reviewed by curriculum co-ordinators and disseminated through curriculum meetings / staff meetings / training sessions
- KS1 and EYFS are involved in Safer Internet day which is introduced during assemblies and followed up in class.
- E-Safety is embedded throughout the school curriculum and visited by each year group as required, and is specifically taught in Computing sessions in Year 1 and Year 2.

Cyberbullying

Cyberbullying is the use of ICT, particularly mobile phones and the internet, to deliberately upset someone else. The whole school community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Head Teachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off site.

Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications.

There are many types of cyber-bullying:

- Sending mean emails, texts or instant messages.
- Sending neutral messages to someone to the point of harassment.
- Posting hurtful things about someone on social media.
- Spreading rumours or gossip about someone online.
- Making fun of someone in an online chat that includes multiple people.
- Attacking or killing an avatar or character in an online game, constantly and on purpose.
- Pretending to be another person by creating a fake online profile.
- Threatening or intimidating someone online or in a text message.
- Taking an embarrassing photo or video and sharing it without permission.

It is important that we work in partnership with pupils and parents to educate them about Cyberbullying as part of our e-safety curriculum. They should:

- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are being cyber bullied.
- report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998. Data can only be accessed and used on school computers. Staff are aware they must not use their personal devices for accessing any school/ children/ pupil data.

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). We must make sure the information is: used fairly, lawfully and transparently. Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you. These include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

Wider Community

Third party users of school equipment will be advised of the policies, filtering and monitoring that is in place. They will be issued with appropriate usernames and password that will be recorded in the school office on request.

Equal Opportunities

Regardless of ability, gender or cultural background, e-safety is an issue which applies to all staff, children and visitors.

Responding to Incidents

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying and Child Protection Policy.

- Any suspected illegal activity will be reported directly to the HT or a member of the school's SLT
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head or deputy headteacher.
- Breaches of this policy by staff will be investigated by the head teacher. Action will be taken under Croydon's Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct.
- Serious breaches of this policy by pupils will be treated as any other serious breach of conduct inline with school Behaviour Policy. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.
- Minor pupil offences, such as being off-task visiting games or other websites will be handled by the teacher in situ by invoking the school behaviour policy.
- The Educations and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate.