Capenhurst C.E. (Controlled) Primary School
E-Safety Policy

The Acceptable Use of the Internet and related Technologies

This policy has been reviewed and agreed by
staff and governors and will be next reviewed in
February 2021

Policy Author	**Mrs E Ritson**
Policy approved by Governors	_____
Policy due for review	**February 2021**

Policy Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students / pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge including **sexting** (see below under 'Communications' for a more detailed explanation)
- Inappropriate communication / contact with others, including strangers
- **Cyber-bullying** (see below under 'Communications' for a more detailed explanation)
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development of this Policy

This e-safety policy has been developed and reviewed by staff and governors.

Consultation with the whole school community takes place annually in the form of an e-safety information session jointly run by school staff and Cheshire Constabulary.

Should serious e-safety incidents take place, the following external persons / agencies should be informed:

- Cheshire West and Chester ICT Helpdesk (Edsential)
- Safeguarding Children in Education Team

The school will monitor the impact of the policy using:

- A log of reported incidents
- Close supervision of pupils' internet activity
- Online Safety awareness day for all pupils
- Ongoing Online Safety lessons as an integral part of the school's computing curriculum

All staff are made aware of the school Acceptable Use Policies which can be accessed and downloaded via the school's website.

Scope of the Policy

This policy applies to all members of the school community (including staff, students, pupils, volunteers, parents / carers, visitors, governors and community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator / Officer
- regular monitoring of e-safety incident log
- reporting to relevant Governors committee / meeting

Governors are reminded of the Seven Principles of Public Office which forms part of the Code of Conduct each governor signs at the start their term of office and the expectation of professional conduct and confidentiality when sending or receiving emails or information in their capacity as a governor of Capenhurst CE Primary School.

Governors are expected to attend e-Safety training (this might be either in-house or provided by an external agency) on a regular basis to ensure that they keep up-to-date with the advances in technology to which the children have access both in school and at home.

Head teacher and Senior Leaders

The head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.

The head teacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff in line with the Allegations against Staff Policy and LADO Guidance.

E-Safety Coordinator / Officer

The E-Safety coordinator will

- lead on safety issues across school
- take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provide training and advice for staff
- feedback to the Governing Body on any relevant items at governing body meetings
- provide Governors with information on how to access online safety training
- liaise with the Local Authority
- liaise with the Local Authority ICT technical staff
- receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meet with the E-Safety Governor to discuss current issues and review incident log

Technical staff

School buys into the Local Authority ICT Support through the SBSA. A technician visits the school on a fortnightly basis offering advice and support which may include the following:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed

Teaching and Support Staff

All staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Acceptable Use Policy
- they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation and possible action
- digital communications with pupils (email / blog / Virtual Learning Environment (VLE)) should be on a professional level and only carried out using official school systems
- use of school laptop for personal Purchasing goods and services during non-contact time falls under 'personal use' of electronic resources. Take advice from your line manager ***before*** you proceed. Internet Banking facilities should not be accessed whilst using a School connection.
- when sending e-mails from a school e-mail address or when using school laptops for personal use, they will ensure that they are mindful of their obligations under the Teachers' Standards,

paying particular attention to Part Two Standards for Personal and Professional Conduct which states that

- Teachers must have proper and professional regard for the ethos, policies and practices of the school in which they teach;

- Teachers must have an understanding of, and always act within, the statutory frameworks which set out their professional duties and responsibilities.

Designated Safeguarding Lead

The designated safeguarding lead should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils

Pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy (AUP), which they will be expected to sign upon entry to school. This will be reviewed on an annual basis.

Parents / Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will take every opportunity to help parents understand relevant e-safety issues through parents' evenings, newsletters, letters and the school website / VLE. Parents and carers will be responsible for:

- endorsing (by signature) the relevant Pupil Acceptable Use Policy

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- Key e-safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of information
- Through the school's computing curriculum
- Through annual Safer Internet Day activities

Education – parents / carers

Parents and carers sometimes either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. “There is a generational digital divide”. (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- The school website
- Letters, newsletters
- Parents’ evenings
- E-Safety Information sessions for parents/carers and pupils run in conjunction with Cheshire Police
- Advice provided on specialist online safety websites, links to which can be found on the school’s website

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. In the main, this will be covered when staff complete their Safeguarding Basic Awareness Training Level 1. Additional information will be shared through e-mails and an e-safety file which will be accessible to all staff. It is the responsibility of each member of staff to read this on a regular basis.

Staff will receive regular in-house training led by the E-Safety Co-ordinator on how to help children stay safe online both in school and outside school.

All staff will be required to complete a computer-based self-assessment regularly to check their level of e-safety awareness and to assess individual training needs. The E-Safety Co-ordinator is responsible for tracking staff training needs in the area of online safety and putting the necessary training provision in place.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. School is supported in this by being part of the Local Authority Internet provision. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password by the ICT co-ordinator who will keep an up to date record of users and their usernames.
- The “master / administrator” passwords for the school ICT system, used by the ICT Technician must also be available to the head teacher or other nominated senior leader and kept in a secure place (e.g. school safe). A school should never allow one user to have sole administrator access.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

Use of digital and video images - Photographic, Video

Staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims with the proviso that the images are stored only within the school server and not taken away from the school premises.

Data Protection

School has a comprehensive GDPR Data Protection Policy which complies with the requirements of the General Data Protection Regulation (GDPR) and which has been read and ratified by Staff and Governors.

In accordance with this policy, personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the Data Protection Act 2018.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- When they are away from their computers they ensure they are locked.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software

School has an appointed Data Protection Officer (DPO) who has been appointed in accordance with the terms set out in section 5 of the school’s GDPR Data Protection Policy which can be accessed and downloaded from the school’s website. The DPO is supported by the head teachers, bursar and Governors of the school.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

- 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 during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- The official school email service may be regarded as safe and secure and is monitored by the Local Authority.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.
- Members of staff at the School should not be interacting with students within a closed, or semi-closed environment. (e.g. 'Closed' communications: Instant Messaging, Personal Email, Direct Messages, etc. 'Semi-closed' communications: Writing on a 'wall' within Facebook, communicating with someone who 'protects' their updates on Twitter, etc.)
- Online interaction within an 'open' online environment *may* be appropriate, if in doubt, staff should consult their line manager for advice.

- 'Open' communications: Blog comments, standard Twitter updates, wikis, etc. Communications with students should be appropriate to your professional remit ***only.***

- Staff social networking profile should be completely unavailable and staff should make any avatars 'appropriate'.

- 'Groups' you join on social networking sites may be seen. Make sure they and any public comments you make reflect positively on you and your profession. Make sure any groups you join cannot have racist, sexist or any other inappropriate overtones

Sexting

Sexting is taking and sharing a nude, partially nude or sexually explicit image or video. If the person in the image or video is under-18, then they are breaking the law. The Protection of Children Act states that it is illegal to create, distribute or possess an indecent image of a child, including self-generated images (e.g. selfies).

All incidents of sexting should be responded to in line with the school's safeguarding policy.

When an incident of sexting comes into school or is brought to the school's attention, the following will happen:

- the incident will be referred to the designated safeguarding lead as soon as possible
- the DSL will hold an initial review meeting with the appropriate school staff
- the children involved will be interviewed (if appropriate)
- parents will be informed at an early state and involved in the process unless there is good reason to believe that informing parents/carers would put the child at risk of harm
- if at any point in the process there is a concern that the child has been harmed or is at risk of harm, a referral will be made to social care and/or the police immediately.

Cyberbullying

Cyberbullying, or online bullying, can be defined as the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else. It is often linked to discrimination, including on the basis of gender, race, faith, sexual orientation or special educational needs and disabilities. Like other forms of bullying, cyberbullying affects the victim's self-esteem and self-confidence and can affect their mental health and well-being.

It can take any different forms: threats and intimidation; harassment or stalking (e.g. repeatedly sending unwanted texts or instant messages); defamation; peer rejection; impersonation and the forwarding or publically posing private information or images.

All incidents of cyberbullying should be responded to in line with the school's safeguarding policy.

When an incident of cyberbullying comes into school or is brought to the school's attention, the following will happen:

- the incident will be referred to the designated safeguarding lead as soon as possible
- the DSL will hold an initial review meeting with the appropriate school staff
- the children involved will be interviewed (if appropriate)
- parents will be informed at an early state and involved in the process unless there is good reason to believe that informing parents/carers would put the child at risk of harm
- if at any point in the process there is a concern that the child has been harmed or is at risk of harm, a referral will be made to social care and/or the police immediately.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

All such incidents will be reported to the appropriate body with the LA. There will be a record kept of any such incident in school.

Schedule for Monitoring and Review

This e-safety policy was approved by the Governing Body in February 2020.

The implementation of this e-safety policy will be monitored by the: E-Safety Coordinator

Monitoring will take place at regular intervals: Once a year

The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) once a year.

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date is February 2021.