



E-Safety Policy

Policy Type:	School (not statutory)
Review Frequency:	Every 3 years
Delegated to:	Curriculum & Pupils' Issues Committee
Last Reviewed/Approved:	May 2024
Policy reviewed by:	Pastoral Deputy Headteacher – Mrs A Williams
	Sponsor Governor – Mr B McAnenny
Date of Next Review:	Summer 2027

RATIONALE

The school's mission statement clearly states that this is a school where we aim for all to feel safe and valued. Under the 2002 Education Act the school has a responsibility to create and maintain a safe learning environment for young people; to identify where there are child welfare concerns and to take action to address such concerns in partnership with other organisations where appropriate ('Keeping Children Safe in Education' 2020, updated January 2021). One important aspect of this in a technological environment where students and staff have ready and frequent access to ICT systems both in and out of school is the area of e-safety. The school recognises its responsibility for providing education and procedures to keep staff and students safe with regard to modern technologies.

PURPOSE

The purpose of the policy is:

- To establish the ground rules we have in school for using ICT equipment and the internet
- To ensure that all who have specific responsibilities regarding e-safety within the school are aware of the scope of those responsibilities
- To highlight the school's commitment to providing e-safety education to staff, students and parents
- To state the ways in which e-safety education will be delivered
- To state the way in which concerns raised regarding e-safety will be addressed whether the concern be around students, staff or others
- To link to other related policies such as freedom of information, data sharing, CCTV, anti-bullying, behaviour, photography and safeguarding as appropriate

CONTEXT

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The internet and other digital/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. This e-safety policy will help to ensure safe and appropriate use.

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 or 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
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- 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 read and used in conjunction with other school policies; specifically, Anti-Bullying, Behaviour for Learning and Child Protection/Safeguarding.

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 provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. This policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

GUIDELINES

This policy applies to all members of the school community (including staff, students, governors, volunteers, parents/carers and visitors) who have access to and are users of school ICT systems, both in and out of school. The school, to such extent as is reasonable, has the responsibility to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary sanctions 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 & Responsibilities

Governors

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. As the Safeguarding Governor, the Chair of Governors will also act as the E-Safety Governor. The role of the E-Safety Governor will include:

- Meetings with the E-Safety Coordinator
- Regular monitoring of e-safety incident logs
- Monitoring of filtering logs
- Reporting to relevant Governors and/or committee(s) meetings.

Senior Leadership Team (SLT)

The Headteacher is responsible for ensuring:

- The safety (including e-safety) of all members of the school community, although the day to day responsibility for e-safety may be delegated to the E-Safety Coordinator
- Adequate training is provided
- Effective monitoring systems are set up
- That relevant procedures, in the event of an e-safety allegation, are known and understood
- Establishing and reviewing the school e-safety policies and documents (in conjunction with E-Safety Coordinator)
- The school's Designated Safeguarding Lead should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of ICT.

E-Safety Coordinator

The E-Safety Coordinator takes day to day responsibility for e-safety issues and has a leading role in:

- Liaising with staff, the LA, ICT Technical staff, E-Safety Governor and SLT on all issues related to e-safety
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Providing training and advice for staff, students and parents
- Receiving reports of e-safety incidents and maintaining a log of incidents to inform future e-safety developments;
- Co-ordinating and reviewing e-safety education programmes in school

Technical Services Manager

The Technical Services Manager is responsible for ensuring that:

- The school's ICT infrastructure is secure and meets e-safety technical requirements
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Technical Services Manager keeps up to date with e-safety technical information
- The use of the school's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Coordinator and/or SLT for investigation/action/sanction.

Teaching & Support Staff

In addition to elements covered in the Acceptable Use Agreement, all teaching and support 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 agreed to the school Staff Acceptable Use Agreement (AUA)
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the school's e-safety and Acceptable Use Agreement
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- In lessons where internet use is pre-planned, students 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.

Students

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Agreement, which they will be required to agree to before being given access to school systems. Parents/carers are required to read through the e-safety section in their child's planner and sign alongside their child's signature
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy also covers their actions out of school, if related to their membership of the school

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. The school will take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Confirming acceptance of the school's Acceptable Use Policy/e-safety rules when they complete the new student registration form.
- Signing the relevant e-safety section of the student planner
- Ensuring their child understands the e-safety rules as part of the acceptable use agreement
- Continuing to support their child in using the school's ICT facilities and the internet in a safe and appropriate way.

Community Users

Community users who access school ICT systems/website/Learning Platform as part of the Extended School provision will be expected to agree to an AUA before being provided with access to school systems.

Education and Training

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

- A planned e-safety programme is provided as part of the form tutor and assembly programme and is regularly revisited in Information Technology and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school
- Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information
- Students are helped to understand the need for the AUA and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside of school
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Rules for the use of ICT systems and the internet are posted in school
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

User Agreement

Anyone accessing the school's IT network must confirm that they accept the on-screen user agreement prior to logging in.

Acceptable Use Policy (Students)

There is an acceptable use policy and agreement in place for students. Parents are expected to read this policy and agreement and make sure that their child understands and abides by the rules. It can

be found in the student planner/handbook and on the following page of the school website: <https://www.clrchs.co.uk/wp-content/uploads/2024/02/Acceptable-Use-Policy-for-Students.pdf>

Acceptable Use Policy (Staff)

There is an acceptable use policy and agreement in place for staff. All staff are expected to abide by this policy, which can be accessed via the staff shared area:

T:\School_Management_Documents\Policies Procedures & Guidance

Copyright

- Students are taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations- staff to monitor this
- Students are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- If using a search engine for images – staff / students should open the selected image and go to its website to check for copyright.

Staff Training

- E-Safety Coordinator ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- A planned programme of e-safety training is available to all staff. An audit of the e-safety training needs of all staff will be carried out annually.
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy, Acceptable Use Agreement and Child Protection Policy
- The E-Safety Coordinator/SLT link will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released
- Governors are invited to take part in e-safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, e-safety, health and safety or child protection.

Communication

Email

- Digital communications with students (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official school systems
- The school's e-mail service should be accessed via the provided web-based interface or Outlook
- Under no circumstances should staff contact students, parents/carers or conduct any school business using their own personal e-mail addresses
- School e-mail is not to be used for personal use. Staff can use their own email in school (before, after school and during lunchtimes when not working with children) – but not for contact with parents/ students.

Mobile Phones

- School mobile phones should be used to contact parents/carers/students when on school business with students off site. Staff should not use personal mobile devices unless it is not possible or practical to use the school mobile.
- Staff should not use personal mobile phones in school during working hours when in contact with children other than for school business such as reading and responding to school emails.

- Students should adhere to the rules and guidelines set out in the policy regarding mobile phone use in school: <https://www.clrchs.co.uk/wp-content/uploads/2022/03/Mobile-Phone-Policy-2021-24.pdf>

Social Networking Sites

- Young people will not be allowed on social networking sites at school; at home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites
- Staff should access social networking sites using personal equipment outside of school hours
- Staff users should not reveal names of staff, students, parents/carers or any other member of the school community on any social networking site or blog
- Students/parents/carers should be aware the school will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders
- If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary
- Students will be taught about e-safety on social networking sites

Digital Images

- The school record of parental permissions granted/not granted must be adhered to when taking images of our students. Names can be obtained from Heads of Year
- Under no circumstances may images of pupils be taken, stored or processed in any way using privately owned equipment.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The school has an active website, Facebook page and twitter account which are all used to inform, publicise school events and celebrate and share the achievement of students.

Removable Data Storage Devices

All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before being run, opened or copied/moved on to local/network hard disks.

Websites

In lessons where internet use is pre-planned, students 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.

- Staff will preview any recommended sites before use
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. Parents will be advised to supervise any further research
- All users must observe copyright of materials published on the internet
- All staff and students are aware that all internet use at school is tracked and logged

The school only allows the E-Safety Co-ordinator, Technical Services Manager, safeguarding team and SLT to access to Internet logs.

Passwords

Staff

All staff must:

- Choose strong passwords which are:
 - at least 8 characters long including a mix of numbers and uppercase and lowercase letters
 - changed on a regular basis [at least every 180 days];
 - not the same as previous passwords used;
 - not obvious or easily guessed (e.g., birthdays or other memorable dates, memorable names, events, or places etc.)
- keep passwords secret;
- never reuse a password;
- never allow any other person to access the school's systems using their login details;

Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct (refer to the Electronic Information & Communications Policy and Information Security Policy).

If given access to the School e-mail system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off when they are leaving the terminal unattended, or when leaving the office, to prevent unauthorised users accessing the system in their absence. Staff should be aware that if they fail to log off and leave their terminals unattended, they may be held responsible for another user's activities on their terminal in breach of policy (refer to the Electronic Information & Communications Policy).

You should not use the same password on multiple systems or attempt to "synchronise" passwords across systems, nor use school passwords for non-work-related purposes.

You should not write down passwords unless stored securely, e.g. in a locked drawer or in a secure password database.

Passwords should **NEVER** be left on display for others to see.

Students

- Should not share their passwords with others
- Should inform staff immediately if passwords are traced or forgotten. ICT Technical staff are able to access the network to allow students to change passwords

Use of Own Equipment

Privately owned ICT equipment should not be connected to the school's network without the specific permission of the Headteacher or Technical Services Manager.

- Students should not bring in their own equipment unless asked to do so by a member of staff.

Use of School Equipment

- No personally owned applications or software packages should be installed on to school ICT equipment
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted
- All should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously or WINDOW L) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Filtering and Monitoring

All use of the school's Internet access is logged and the logs are randomly but regularly monitored by the school safeguarding team. Whenever any inappropriate use is detected, it will be followed up by the E-Safety Co-ordinator, SLT or members of the safeguarding team depending on the severity of the incident.

E-Safety Coordinator, Technical Services Manager and the safeguarding team will maintain the ICT Log and record any breaches, suspected or actual, of the filtering systems. Any member of staff employed by the school who comes across an e-safety issue should immediately report it to the E-Safety Co-ordinator or safeguarding team and confiscate the equipment where able. This is part of the school safeguarding protocol (if the concern involves the E-Safety Co-ordinator then the member of staff should report the issue to the Headteacher).

We filter for:	<ul style="list-style-type: none"> • Illegal activity • Self-harm and suicide • Bullying • Substance misuse • CSE • Sexual harassment • Pornography • Extremism • Profanities
We monitor by:	Our Smoothwall Internet Filter logs anything searched for on the internet and will block websites belonging to these categories
When inappropriate usage is detected:	An Impero alert is sent to key members of staff – IT team, E-Safety Coordinator and SLT members of the Safeguarding Team. It is reviewed and forwarded to appropriate teams for action (SEND, PALS, etc.)
We record our concerns on:	Synergy and/or CPOMS
We would escalate to local safeguarding partners when:	A child's safety has been compromised and we need external support for the victim and/or family; a child is at risk of CSE, CCE or radicalisation; a child has distributed indecent content
The responsibility staff have in relation to this is	<p>Embed e-safety issues in all aspects of the curriculum and other school activities</p> <p>Supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)</p> <p>Ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws</p>

Incident Reporting

Any e-safety incidents must be immediately reported to the Headteacher (if a member of staff) or the E-Safety Coordinator/safeguarding team (if a student) who will investigate further following e-safety and safeguarding policies and guidance.

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. Any apparent or actual incidents of misuse will be dealt with in the most appropriate manner. If any apparent or actual misuse appears to involve illegal activity e.g. child sexual exploitation images, adult material, criminally racist material or other criminal conduct, activity or materials, the LA (and maybe police) will be contacted. Actions will be followed in accordance with this policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might



have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation. It is likely that the school, as opposed to police, will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

Linked documents:

- Child Protection & Safeguarding Policy & Procedures
- Keeping Children Safe in Education
- Guidance for Safer Working Practice

- Acceptable Use Agreement for Staff
- Acceptable Use Agreement for Students
- BYOD Policy
- Cyber Security Policy
- Electronic Information & Communications Policy
- Home Working Policy
- Information Security Policy
- Social Media Policy
- Mobile Phone Policy
- Photography & Digital Images Policy

Policy Approval:

Signature of Headteacher:		Date:	11.06.2024
Signature of Chair/Vice-Chair of the C&P Committee		Date:	11.06.2024