E-Safety Policy

Introduction

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.

However, the use of these new technologies can put young people at risk within and outside the school. These can be categorised into four types:

content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying;

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

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 (eg 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. Termly E-safety lessons form part of the ICT curriculum.

Scope of the Policy

This policy applies to all members of the school community including EYFS, who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headmasters, 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.

This policy should be read in conjunction with KCSIE 2021 as well as the safeguarding, anti-bullying and remote learning policies.

Roles and Responsibilities

The Headmaster 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 Head of ICT.
- ensuring that the Head of ICT and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- ensuring that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role

The Head of ICT is responsible for ensuring

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's networks through a properly enforced password protection policy
- the school's filtering policy is applied and updated on a regular basis.
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- Running e-safety training on a regular basis for staff and parents as well as ensuring it is embedded in the curriculum. This includes time at Inset meetings and yearly evening presentations to parents.
- an effective system for remote learning is in place

The Designated Safeguarding Lead is responsible for

- ensuring an effective e-safety curriculum is in place
- ensuring an effective filtering system is in place

- ensuring an effective system is in place for mobile technology
- responding to any safeguarding issues flagged up by the automated filtering system
- responding to any concerns raised by parents, pupils and staff

Teaching and Support Staff are responsible for ensuring that:

- they report any suspected misuse or problem to the Head of ICT
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils 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
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned 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
- they are aware of the risks of radicalisation

Pupils should

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. This includes understanding that mobile (3G, 4G or 5G) access is turned off whilst in school or on school trips
- know and understand school policies on the taking / use of images, in particular that they should not be taking images or videos of other pupils unless it is part of a supervised lesson.
- know and understand what cyber-bullying is and how to recognise and deal with any issues arising from it
- Understand how to raise concerns
- 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 covers their actions out of school, if related to their membership of the school
- Understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults.

- know and understand how to use remote learning systems safely

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:

- A planned e-safety programme is part of ICT lessons and is regularly revisited – this covers both the use of ICT and new technologies in school and outside school
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be taught what to do if they come across inappropriate material and who they should raise concerns with
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- When working remotely, pupils must :
    - Be contactable during the school day in line with their timetable
    - Complete work to the deadline set by teachers
    - Seek help if they need it, from teachers or teaching assistants
    - Alert teachers if they're not able to complete work
    - Work in communal areas of the house

Education – parents/carers

E-safety information for parents can be found on the school website. Annual evening meetings are also held to brief parents on e-safety.

Staff can expect parents with children learning remotely to:

Make the school aware if their child is sick or otherwise can't complete work

Seek help from the school if they need it

Technical

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers must be securely located and physical access restricted

- All users will have clearly defined access rights to school ICT systems.
- All users (from reception and above) will be provided with a username and password by the Head of ICT 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 Head of ICT must also be available to the Headmaster and kept in a secure place (eg school safe)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- In the event of the Head of ICT needing to switch off the filtering for any reason, or for any user, the Headmaster must be notified
- Ensuring the web filter is kept up to date and that reports are generated and checked for inappropriate sites by the Head of ICT. Any safeguarding reports are automatically generated for the DSL.
- The filter comprises both user based filtering and a transparent proxy for other devices, managed by RM. Any visitors granted access to the school’s wifi will have internet access filtered through the transparent proxy.
- 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.
- Pupil data cannot be transferred onto unencrypted devices or taken off site under any circumstances

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 using age appropriate resources

.

- in lessons where internet use is pre-planned, it is best practice that 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 pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should understand the risks posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults

Useful resources can be found at:

- Professionals Online Safety Helpline (https://www.saferinternet.org.uk/helpline/professionals-online-safety-helpline)
- Reporting Harmful Content (https://www.saferinternet.org.uk/helpline/report-harmful-content)

- CEOP (https://www.ceop.police.uk/ceop-reporting/)
- Internet Watch Foundation. (https://report.iwf.org.uk/en)

The Head of ICT is also a CEOP ambassador

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, 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 eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images must only be taken on school equipment
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without both their permission and the permission of the school.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- In the EYFS, children have their photographs taken to provide evidence of their achievements for developmental records (The Early Years Foundation Stage, EYFS 2012). Staff, visitors, volunteers and students are not permitted to use their own mobile phones, tablets or cameras to take or record any images of children for their own records during session times but instead must use the school cameras or tablets purchased or provided for the purpose. Staff may take photographs of children in the EYFS setting using a school camera or tablet for the following purposes: in order to provide evidence of any practical educational activities or outdoor learning that has taken place during the day, or on school trips to document their outing for newsletters and for their learning journey. Staff must regularly delete all photos and videos from such devices.

Data Protection

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.
- Only store any personal data in designated folders on the school network
- Only 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 data must be encrypted and password protected
    - **t**he 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
    - the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete
    - the data must not be transferred to any personal devices

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- 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 pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils will be provided with individual school email addresses for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Pupil Acceptable Use Policy

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger" and will not disclose or share personal information about myself or others when on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping or file sharing
- I will not access video broadcasting sites (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will not access, copy, remove or otherwise alter any other user's files, without their permission.
- I will be polite and responsible when I communicate with others, respecting their views
- I will not take, distribute or publish images or videos of anyone without both their permission and the permission of the school.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- Mobile devices should be stored in the School Office or in the boarding wing during the day. They may be used on minibuses as per the minibus policy.
- 3G, 4G and 5G connectivity must be turned off at all times (airplane mode)
- Usage of mobile devices in the evening is governed by the boarding handbook
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent it

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only use age appropriate chat and social networking sites and, even then, only with permission

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

When working remotely:

- I should only contact staff through the school's email system or Google classrooms
- Be contactable during the school day in line with their timetable
- Complete work to the deadline set by teachers
- Seek help if needed from teachers or teaching assistants
- Alert teachers if not able to complete work
- Work in communal areas of the house
- Be polite any courteous when messaging any member of the school community

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Signed:

Signature of Parent/Guardian:

Date:

Staff (and Volunteer) Acceptable Use Policy

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use anyone else's.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images under any circumstances. Where these images are published (eg on the school website / VLE) it should not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has a responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use a personal device in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software
- I will not open any attachments to emails, unless the source is known and trusted
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, without prior agreement from the Head of ICT.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I will not store pupil personal data on any personal devices
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, termination of contract and in the event of illegal activities the involvement of the police.

Policy Last Reviewed	Autumn 2021
Policy Next Reviewed	Autumn 2024
Staff Responsible	Head of ICT
Governor Review	Ed committee – Autumn 2019
ISI Reference	n/a
Website	Yes