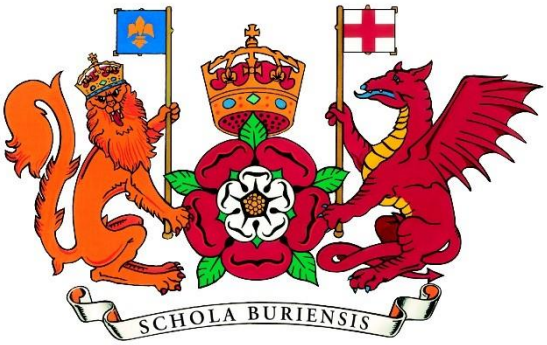

Curiosity | Care | Courage | Creativity

King Edward VI School

Online Safety Policy

(includes Acceptable Use of IT and Mobile Phones Policy)

January 2024

Our Vision:
To be a vibrant learning community nurturing courage, care, curiosity and creativity in every young person, so that they flourish in the world with hope and self-belief.

Version Number:	Version 1
Drawn up by:	Tom Spillane Assistant Headteacher
Reviewed by:	SLT
Date reviewed:	January 2024
Approval by:	Curriculum & Standards Committee Full Governing Body
Date approved:	27 March 2024
Review Cycle:	1 Year
Date of next Review:	January 2025

Contents

1. Purpose

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **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**: 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, and

- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your students, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

(In line with Keeping Children Safe in Education – September 2023)

1.1 Principles

- New technologies have become integral to the lives of children and young people in today's society, both within school 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 students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people have an entitlement to safe internet access at all times

- The use of these exciting and innovative tools in school and at home has been shown to help raise standards and promote student 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
    - Inappropriate communication/contact with others, including strangers
    - Online bullying

- Promoting illegal acts
- 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 online safety policy is used in conjunction with other school policies (eg Behaviour, and Safeguarding policies)

- As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' 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 done everything that could reasonably be expected to manage and reduce these risks.

1.2 Scope
This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, 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 Headteachers, to such extent as is reasonable, to regulate the behaviour of students 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 bullying or other online 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 antibullying policies and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

2. Roles and Responsibilities
The Online Safety Team for academic year 2023/24 is:

Online Safety Lead & Designated Safeguarding Lead – Tom Spillane
IT Manager – Stuart Whiting
PSHE Co-ordinator – Sara Pickett
Online Safety Governor – Jon Swift

The roles and responsibilities for online safety of individuals and groups within the school:

2.1 Governors:
- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body will take on the role of Online Safety Governor

- The role of the Online Safety Governor includes regular meetings with the Online Safety Lead and the school's Designated Safeguarding Leads to discuss current issues and monitor online incidents

- The Governing Body is responsible for ensuring that its employees act in a lawful manner, making appropriate use of school technologies for approved purposes only

- The Governing Body is responsible for adopting relevant policies and the Headteacher for ensuring that staff are aware of their contents.

2.2 Headteacher and Senior Leaders

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community

- The Headteacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable CPD to enable them to carry out their role and to train other colleagues, as appropriate

- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles

- The Headteacher and members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious allegation being made against a member of staff

- The Headteacher is responsible for maintaining an inventory of IT equipment and a list of school laptops and mobile phones and to whom they have been issued

- If the Headteacher has reason to believe that any IT equipment has been misused, they should consult the HR Manager for advice without delay. Incidents will be investigated in a timely manner in accordance with agreed procedures.

- Headteachers should make it clear that internal school staff should not carry out any investigations unless they are both qualified and authorised to do so

2.3 Online Safety Lead

- Takes day to day (managed by the school's Designated Safeguarding Leads) responsibility for online issues and has a leading role in establishing and reviewing the school policy

- Ensures that all staff are aware of the procedures that need to be followed in the event of an online incident taking place

- Provides training and advice for staff

- Liaises with the IT Manager

- Receives reports of online incidents and ensures a log is kept of incidents to inform future developments

- Meets regularly with the Online Safety Governor and Designated Safeguarding Leads to discuss current issues and review incidents

- Reports to the school's Designated Safeguarding Leads.

2.4 IT Manager/IT Support Staff are responsible for ensuring

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack

- That the school meets online safety technical requirements

- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed

- That they keep up to date with online safety technical information in order to effectively carry out their role and to inform and update others as relevant

- Regular monitoring of internet/change control logs and reporting to Online Safety Lead/Senior Leaders as appropriate

- That the use of the school's network, remote access and email is regularly monitored in order that any misuse/attempted misuse can be reported to the IT Manager who would then refer on as appropriate to either the Online Safety Lead or Senior Leaders.

2.5 Teaching and Support Staff are responsible for ensuring that

- They have an up-to-date awareness of online safety matters and of the current school policy and practices

- They have read, understood and signed the school Acceptable Use of ICT & Mobile Phones Policy

- They report any suspected misuse or problem to the IT Manager/Online Safety Lead for investigation and action

- Digital communications with students (email/internet based) should be on a professional level and only carried out using official school systems

- Online safety issues are embedded in all aspects of the curriculum and other school activities

- Students understand and follow the school Online Safety and Acceptable Use policy

- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- They monitor IT activity in lessons, extra-curricular and extended school activities

- They are aware of online safety issues related to the use of mobile phones, watches, 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 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.

- In class use of mobile phones/devices is controlled by the classroom teacher.

2.6 Designated Safeguarding Lead

Should be trained in online 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
- Online bullying.

2.7 Students are responsible for using the school IT systems in accordance with the IT Agreement, which they will be expected to sign before being given access to school systems:

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policy on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policy on the taking/use of images and on online bullying
- Should understand the importance of adopting good online practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

2.8 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 IT than their children. The school will therefore take every opportunity to help parents/carers understand these issues through consultation evenings, newsletters, letters, website and information about national/local online safety campaigns/literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Student IT Agreement
- Accessing the school website/online student records in accordance with the relevant School Acceptable Use Policy

3. Education

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

Online safety education will be provided in the following ways:

- Key online safety messages will be reinforced in assemblies and tutorial activities
- Students should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information

- Students should be encouraged to adopt safe and responsible use of IT, the internet and mobile, watches and handheld devices both within and outside school

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Staff should act as good role models in their use of IT, the internet and mobile, watches and handheld devices.

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

- Information evenings

- Individual conversations

- Newsletters and other suitable material.

4. Technical – infrastructure, equipment, filtering and monitoring

To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems

- review filtering and monitoring provision at least annually

- block harmful and inappropriate content without unreasonably impacting teaching and learning

- have effective monitoring strategies in place that meet their safeguarding needs.

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 IT systems will be managed in ways that ensure that the school meets the online safety technical requirements

- There will be regular reviews and audits of the safety and security of school IT systems

- Servers, wireless systems and cabling will be securely located and physical access restricted

- All users will have clearly defined access rights to school IT systems this is reviewed according to changing requirements

- All users will be provided with a username and password

- The ‘master/administrator’ passwords for the school IT system, used by the IT Manager will also be available to the Headteacher and kept in a secure place

- 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

- The school maintains internet filtering provided by McAfee

- In the event of the IT Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher

- Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager/IT support staff

- School IT support staff regularly monitor and record the activity of users on the school IT systems and users are made aware of this in the Acceptable Use section of this policy

- Remote management tools are used by the IT Manager/IT Support Staff to control workstations and view user's activity, this includes keyword monitoring functionality

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data

- The school infrastructure and individual workstations are protected by up to date antivirus software.

5. Curriculum

- In lessons where internet use is pre-planned, it is best practice that 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

- Where students are allowed freely to search the internet, staff should be vigilant in monitoring the content of the websites that students visit

- It is accepted that from time-to-time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Manager or IT Support Staff temporarily remove those sites from the filtered list for the period of study. Any request to do so should be in writing with clear reasons for the need

- Students should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

6. Use of digital and video images

- When using digital images, staff should inform and educate students 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, but must follow school policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes

- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute

- Students must not take, use, share, publish or distribute images of others without their or their parent/carer's consent

- Students' names/photographs will not be used online without consent from their parent/ carer's consent. Permission is obtained on admission to the school.

7. Data Protection/GDPR

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and in line with current GDPR.

8. Social Media

The widespread availability and use of social media applications such as Facebook and Twitter, bring opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our school, the community, our legal responsibilities and our reputation. To capture the benefits offered by social media, the School may explore and implement its use for school improvement and educational purposes.

Working in a school, requires us all to maintain professional boundaries in all forms of communication whether or not it involves electronic/digital technology. This is vital to maintain public trust and appropriate professional relationships with students. Our conduct inside or outside of work should not lead us to blur or cross those professional boundaries.

This policy and the principles below are to help staff and individuals avoid the downside risks of using social media. The principles apply to any approved use of social media communication within the school or to personal use of social media outside of school.

9. Application

This document applies to all staff, including agency/supply staff, volunteers, governors or anyone working within the school and using the school's systems and equipment whether on or off the premises. The policy may also apply to former employees in certain circumstances. The use of the word 'individuals' in this document includes this range of people.

The policy and principles should be read in conjunction with the Staff Code of Conduct.

10. Definition

In this document, social media means electronic communication software, applications (including those running on mobile devices including texting, SMS, and videos), e-mail and web sites, which enable users to interact, create and exchange information online. Examples include, but are not limited to, sites such as Facebook, Twitter, Instagram, YouTube, as well as online discussion forums, blogs, other and the use of webcams. All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of

Information legislation, the Safeguarding Vulnerable Groups Act 2006, the Malicious Communications Act 1988 and other legislation. They must also operate in line with the school's Equalities, Child Protection and Safeguarding policies.

11. Access to Social Media sites using school equipment/systems

With the exception of communication sites created by or approved by the school for internal use, the School does not allow access to social networking websites from its computers or systems within the school day.

12. Key principles when using Social Media sites

There are many legitimate uses of social media within the curriculum and to support student learning. For example, the school has an official Twitter account and courses may require the use of blogs for assessment. There are also many possibilities for using social media to enhance and develop students' learning. However, when using social media, the boundaries between professional and personal can become more blurred and users can unwittingly or wittingly publish things they may later regret. Published items can be capable of more than one interpretation but once published the damage may not be recoverable.

12.1 The golden principles

An individual is under a duty to:

- Maintain proper professional boundaries with students, parents and carers even when students, parents or carers initiate electronic interaction
- Before posting items or communicating in social media to consider seriously whether the item would be said in public or shown in public or written for the public to read. If not, or if there is some doubt then it should not be posted because you may not be able to control who sees the information and how they interpret it
- Be particularly aware of the guidelines when staff have external friendships with parents/carers.

An individual is under a duty not to:

- Disclose confidential information without express authority especially about students, parents or carers, staff, voluntary or other workers at the school nor breach their right to privacy
- Engage in posts or activities which are detrimental to maintaining effective working relationships between individuals 'working' at the school
- Bring the reputation of the school into disrepute
- Engage in activities which compromise, or might be seen to compromise, the professional standards of teaching or the professional standards applicable to support staff
- Share information with students or parents/carers in any environment that they would not willingly and appropriately share in a school or school related setting or in the community
- Post comments which incite others to make discriminatory or other professionally unacceptable comments
- Post school logos or similar images that may lead readers of posts etc. to believe the individual is speaking on behalf of the school.

Items placed on social networking sites will be regarded as having been posted in the public domain. Thus, it is very important to be careful when using social media personally.

We trust that the advice below will help all individuals to avoid falling foul of the golden principles and the points below.

12.2 Effective practices when using social media sites

Members of staff should:

- Use caution when posting information on social networking sites and other online forums
- Consider refraining from identifying themselves as working for the school as posted content could bring the school into disrepute
- Take care that their interaction on social media does not damage working relationships between members of staff, students at the school, their families and other stakeholders and/or working partners of the school
- Maintain professional standards by communicating with student & parents/carers electronically at appropriate times of the day and through established education platforms (for example, a web page dedicated to school programme, project or class rather than via a personal profile)
- Avoid exchanging private texts, phone numbers, personal email addresses or photos of a personal nature with students/parents or carers
- Decline student initiated 'friend' requests and not issue 'friend' requests to students nor communicate with students on any social network site or similar website or forum
- Maintain a formal, courteous and professional tone in all communications with students to ensure that professional boundaries are maintained
- If posting an item about an aspect of the school, for which you have express permission from the Headteacher, make it clear that any personal views are not necessarily those of the school
- Staff should not accept any current student of any age or any ex-student of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account.
- Manage the privacy and security settings of your social media accounts. Privacy settings can shift and change without notice. Check the settings frequently.
- Ensure that privacy settings for content/photos are set appropriately and monitor who can post to your social media locations and view what you post. You should not allow students to view or post on those locations
- Protect yourself from identity theft by restricting the amount of personal information that you give out. Be cautious about posting detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords and enable personal details to be cloned for fraudulent acts etc and grooming.

12.3 The following activities must not be undertaken:

- Bullying and harassment – such conduct against any colleagues via social media sites is taken as seriously as workplace bullying and harassment. Any allegations will be dealt with under the schools' normal bullying and harassment and/or disciplinary policies and may be treated as a criminal offence in certain circumstances
- Incitement of racial or religious hatred or similar activities – these may lead to criminal investigations and penalties
- Posting libellous statements – an individual may be legally liable for any damage to the reputation of the individual concerned. As a representative of the school, any statement made by an employee could mean the school is vicariously liable for defamatory statements if carried out in the normal course of employment, even if performed without the consent or approval of the school. Similarly, making such statements on your own initiative and not at work could mean you face legal action

- Grooming students or similar activities to develop an inappropriate relationship(s)
- Bring the school's reputation into disrepute
- Compromising the security of the school's systems
- Breaching confidential information about the school or any of its students, staff, governors, volunteers or other individuals associated with the school**.** Don't publish anything that might allow inferences to be drawn which could embarrass or damage a student, employee, governor, volunteer or supplier.
- Breaches of copyright or other similar infringements – passing on text, photos etc; may infringe the owner's copyright. Always ensure that you have the permission of the owner
- The school takes the matters above seriously and disciplinary action will be taken. If substantiated, the normal outcome will be dismissal. A very serious view will also be taken of any individual, who ignores or wilfully or carelessly carries out actions or omits to act which results in breaches of the instructions and advice contained in this policy and the result is for example, undermining effective working relationships, professional boundaries between individuals and student similar examples in this policy.

12.4 Feeling aggrieved or concerned about matters at work

When you feel that unfair decision has been made or that malpractice is occurring what can you do? What you should not do is post your feelings on-line, which are likely to be impulsive, inappropriate or heated comments. Those may lead you into being part of the problem. Instead you can use several routes:

Whistle blowing procedure - for allegations of organisational malpractice or corruption – See *Whistle Blowing* policy on the school website. Following this procedure provides protection against dismissal and other sanctions if you disclose matters in the ways set out in the procedure. Posting comments first will mean you forfeit your legal protection.

Grievance procedure - if you feel aggrieved by a decision at the school that affects you personally.

13. Dealing with inappropriate contact or material/comments

If an individual becomes aware of inappropriate material/comments he/she should notify the Online Safety Lead or the IT Manager as soon as possible, and if possible provide print outs of the comments made.

If a student makes 'social' or inappropriate contact with an employee, the individual must notify the Designated Safeguarding Lead as soon as possible without making a response. Similarly, if any member of staff or individual associated with the school makes unintended contact with a student, the incident must be notified to the Designated Safeguarding Lead as soon as possible. The school can then deal with the situation as appropriate.

Refer to the schools Online Safety section of this policy for more details and/or the Safeguarding Policy if the incident gives rise to potential or actual safeguarding concerns.

14. Responding to incidents of misuse

- It is hoped that all members of the school will be responsible users of IT, 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

- Student misuse will be dealt with through the school's behaviour management procedures, unless there are legal or child protection concerns, in which case the incident will be reported to the relevant outside agencies, such as the police or social services

- Staff misuse will be dealt with through the school and Local Authority's disciplinary procedures.

Acceptable Use of IT and Mobile Phones Policy

This policy applies to all users of school and personal IT equipment/services.

1. User Responsibilities

1.1 Staff found to be in breach of this policy may be disciplined in accordance with the disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in termination of employment. Users must report all suspected breaches of this policy to the Headteacher.

1.2 Users and their managers are responsible for ensuring that adequate induction, training and support is undertaken to implement this policy.

1.3 By logging on to IT systems, users agree to abide by this Acceptable Use policy and other policies that relate to the use of IT.

1.4 All users are expected to act in a responsible, ethical and lawful manner with the understanding that school electronic and manual information may be accessible to the public under the Freedom of Information Act 2000. Users should uphold privacy and confidentiality in accordance with the Data Protection Act 2018. Care must also be taken not to breach another person's copyright, trademark or design, nor to publish any defamatory content.

1.5 Staff who have been given the use of a school laptop will be expected to sign for its use on receipt. Staff may use school equipment for authorised business use only, except as allowed for in paragraph 10.1.

1.6 Staff must follow authorised procedures when relocating IT equipment or taking mobile devices offsite.

1.7 No one may use IT resources in violation of license agreements, copyrights, contracts or national laws, or the Standing Orders, policies, rules or regulations of the school or the County Council.

1.8 Users are required to protect their password and not share their account details with others for their use, nor utilise another users' account or misrepresent their identity for any reason. Users must not under any circumstances reveal their password to anyone else.

1.9 No user shall access (e.g., read, write, modify, delete, copy, move) another user's **personal** electronic documents (including email) without the owner's permission or as allowed by this policy or by law.

1.10 Users must not load or download software on any device without the authorisation of the IT Manager. Periodic audits of software held on IT equipment will be undertaken.

1.11 Users must take care to store sensitive information, e.g. student data safely and to keep it password protected, on all school systems, including laptops & removable storage such as USB drives. Encryption guidance, as provided by the IT team, should be followed at all times.

1.12 Network connected devices must have school approved anti-virus software installed and activated. Users may not turn off anti-virus software. All users of IT resources have the responsibility to take precautions to prevent the initial occurrence and subsequent

spreading of a computer virus. No one may knowingly create, install, run, or distribute any malicious code (e.g. viruses, Trojans, worms) or another destructive programme on any IT resource.

1.13 No one may knowingly or willingly interfere with the security mechanisms or integrity of IT resources. No one may use IT resources to attempt unauthorised use, or interfere with the legitimate use by authorised users, of other computers on internal or external networks. Access to networks will be monitored.

1.14 Within the terms of the Data Protection Act 2018, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the County Council or school may record or inspect any information transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice when:

- There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy
- An account appears to be engaged in unusual or unusually excessive activity
- It is necessary to do so to protect the integrity, security, or functionality of IT resources or to protect the County Council or its partners from liability
- Establishing the existence of facts relevant to the business
- Ascertaining or demonstrating standards which ought to be achieved by those using the
- IT facilities
- Preventing or detecting crime
- Investigating or detecting unauthorised use of IT facilities
- Ensuring effective operation of IT facilities
- Determining if communications are relevant to the business (for example, in the last resort where an employee is off sick or on holiday and business continuity is threatened)
- It is otherwise permitted or required by law.

1.15 Do not send private, sensitive or confidential information by unencrypted email – particularly to an external recipient - if accidental disclosure the data breach must be reported as per GDPR requirements. Redact personal data where possible or anonymise by using initials. Use passwords on sensitive documents that must be sent to external recipients. In accordance with the Data Protection Act (2018).

1.16 Websites/school social media accounts must not be created on school equipment without the written permission of the Headteacher in consultation with the IT Manager.

1.17 No one may use IT resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law. No one may abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a school account.

1.18 The following content must not be created or accessed on IT equipment at any time:

- Pornography and other inappropriate sexual content
- Material that gratuitously displays images of violence, injury or death
- Material that is likely to lead to the harassment of others
- Material that promotes intolerance and discrimination on grounds of race, sex, disability, sexual orientation, religion or age & radicalisation
- Material relating to criminal activity, for example buying and selling illegal drugs

- Material relating to any other unlawful activity e.g. breach of copyright
- Material that may generate security risks and encourage computer misuse.

1.19 It is possible to access or be directed to unacceptable Internet sites by accident. These can be embarrassing and such sites can be difficult to get out of. If staff have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the IT Manager. This may avoid problems later should monitoring systems be alerted to the content.

1.20 School laptops and other equipment are not the school's liability when in the private possession of members of staff, such as at home. Staff are recommended to add such items to their home insurance. Due care must be taken by staff to keep such items safely. In the case of their loss or theft, the School cannot give any guarantee to replace such items.

2. Personal use and privacy

2.1 In the course of normal operations, IT resources are to be used for business purposes only. The school permits limited personal use of IT facilities by authorised users subject to the following limitations:

- Personal use must be in the user's own time and must not impact upon work efficiency or costs
- The level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided
- Personal use must not be of a commercial or profit-making nature
- Personal use must not be of a nature that competes with the business of the school or conflicts with an employee's obligations.

2.2 Personal use of the Internet must not involve attempting to access the categories of content described in section 9.18 that is normally automatically blocked by web filtering software.

3. Mobile phone communication and instant messaging

3.1 Staff must not give their home telephone number or their personal mobile phone number to students. Mobile phone communication should be used sparingly and only when deemed necessary. School mobiles are to be used for trips.

3.2 Photographs and videos of students should not be taken with mobile phones by staff or students except where staff have authorisation for this.

3.3 Staff are advised not to make use of students' mobile phone numbers either to make or receive phone calls or to send to or receive from student's text messages other than for approved school business.

3.4 Staff should only communicate electronically with students/parents or carers from school accounts on approved school business, e.g. coursework.

3.5 Staff should not enter into instant messaging communications with students.

3.6 When Staff use mobile phones in school, this use should be discreet & appropriate.