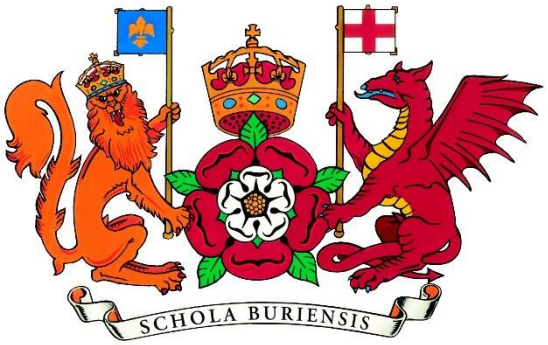


Curiosity | Care | Courage | Creativity

# King Edward VI School

## Online Safety Policy

## (includes Acceptable Use of IT and Mobile Phones Policy)

## February 2025

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 2 |
| **Drawn up by:** | Tom Spillane<br>Assistant Headteacher |
| **Reviewed by:** | SLT |
| **Date reviewed:** | February 2025 |
| **Approval by:** | Curriculum & Standards Committee<br>Full Governing Body |
| **Date approved:** | March 2025 |
| **Review Cycle:** | 1 Year |
| **Date of next Review:** | February 2026 |

**Contents** Page

## 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 to protect and educate the whole school 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**: 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. If you feel your 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 2024)

### 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. Legislation and Guidance**
This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Searching, screening and confiscation

Relationships and sex education

It also refers to the DfE's guidance on protecting children from radicalisation

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

## 3. Roles and Responsibilities

The Online Safety Team for academic year 2024/25 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:

### 3.1 Governors:

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Reviewing filtering and monitoring provisions at least annually.
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Jon swift.

All governors will:

- Ensure they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special

educational needs and/or disabilities (SEND): This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

### 3.2 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.

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

### 3.3 Online Safety Lead

Details of the school's Designated Safeguarding Lead (DSL) and deputies are set out in our Safeguarding Policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly.
- Working with the ICT manager to make sure the appropriate systems and processes are in place.
- Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's child protection policy.

- Responding to safeguarding concerns identified by filtering and monitoring.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Headteacher and/or governing board.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

**3.4 IT Manager/IT Support Staff are responsible for:**

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a regular basis including half termly checks by DSL and or Safeguarding Governor.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

**3.5 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.

**3.6 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.

**3.7 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.

**3.8 Parents/Carers**
Parents/carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre

Online safety topics for parents/carers – Childnet

Parent resource sheet – Childnet

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.

## 4. Education

In **KS3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Students in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.

- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

### 4.1 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.

### 5.1. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or parent bulletins. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use.

- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.
- If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.
- Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

## 6. Cyber-bullying

### 6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's Behaviour Policy.)

### 6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Personal, Social, Health and Economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

## 7. 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.

**8. 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.

**9. Artificial intelligence (AI)**

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

King Edward VI School recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

King Edward VI School will treat any use of AI to bully students in line with our anti bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school

**10. Examining electronic devices**

The Headteacher, and any member of staff authorised to do so by the Headteacher (as set out in the Behaviour Policy) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students and/or
- Is identified in the school rules as a banned item for which a search can be carried out. and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the Headteacher or DSL.
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.

- Seek the student's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Behavior Policy

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

## 11. 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.

### 11.1 Application

This 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.

### 11.2 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.

### 11.3 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.

### 11.4. 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.

### 11.5 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.

**11.6 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.

**11.7 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.

**11.8 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.

## 12. 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.

## 13. 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.

## 14. Training

### 14.1 Staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.

Children can abuse their peers online through:

- Abusive, threatening, harassing and misogynistic messages.
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
- Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

### 14.2 Students

All students will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information.
- Password security.
- Social engineering.
- The risks of removable storage devices (e.g. USBs).
- Multi-factor authentication.
- How to report a cyber incident or attack.
- How to report a personal data breach.

Students will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

## 15. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the Senior Leadership Team. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

## Appendix A

### 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.

**Appendix B:**

**Appendix 5: online safety training audit**

| ONLINE SAFETY TRAINING NEEDS AUDIT | |
|---|---|
| **Name of staff member/volunteer:** | **Date**: |
| **Question** | **Yes/No (add comments if necessary)** |
| Do you know the name of the person who has lead responsibility for online safety in school? | |
| Are you aware of the ways students can abuse their peers online? | |
| Do you know what you must do if a student approaches you with a concern or issue? | |
| Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors? | |
| Are you familiar with the school's acceptable use agreement for students and parents/carers? | |
| Are you familiar with the filtering and monitoring systems on the school's devices and networks? | |
| Do you understand your role and responsibilities in relation to filtering and monitoring? | |
| Do you regularly change your password for accessing the school's ICT systems? | |
| Are you familiar with the school's approach to tackling cyber-bullying? | |
| Are there any areas of online safety in which you would like training/further training? | |

**Appendix C: online safety incident report log**

| ONLINE SAFETY INCIDENT LOG | | | | |
|---|---|---|---|---|
| **Date** | **Where the incident took place** | **Description of the incident** | **Action taken** | **Name and signature of staff member recording the incident** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |