

Online Safety Policy

This policy adopted	July 2025
Next review date	July 2027
Approved by	Headteacher
Statutory	No

Table of Contents

1. Aims.....	3
2. Legislation, guidance and links to other policies.....	3
3. Roles and responsibilities	4
3.1 The governing board.....	4
3.2 The headteacher and senior leaders	5
3.3 The designated safeguarding lead.....	5
3.4 The SLT lead for IT	6
3.5 The IT strategic lead	6
3.6 All staff and volunteers.....	7
3.7 Parents.....	8
3.8 Visitors and members of the community.....	8
3.9 Students	8
4. Educating pupils about online safety.....	9
5. Educating parents about online safety	9
6. Cyber-bullying.....	9
6.1 Definition.....	9
6.2 Preventing and addressing cyber-bullying	9
6.3 Examining electronic devices	10
7. Acceptable use of the internet in school.....	10
8. Pupils using mobile devices in school	10
9. Staff using personal devices	11
10. How the school will respond to issues of misuse	11
11. Training.....	11
12. Monitoring arrangements.....	12
Appendix 1: Student Acceptable Use Agreement	13
Appendix 2: Staff Acceptable Use Agreement.....	15

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as ‘mobile phones’)
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

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

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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

2. Legislation, guidance and links to other policies

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](#)
- [Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff](#) [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

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 pupils' electronic devices where they believe there is a 'good reason' to do This policy complies with our funding agreement and articles of association.

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

3. Roles and responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals¹ and groups within the school.

3.1 The governing board

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

The DfE guidance "Keeping Children Safe in Education" states:

"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare this includes ... online safety"

"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy [e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body"](#).

- The governing board will receive termly updates about online safety as part of the Governors' Report. This will include information on reports of online safety incidents, reviewing filtering and monitoring, , and reviewing progress towards the digital standards.
- Ensure that 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 or college 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

pupils 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

- There will be regular meetings with the online safety lead and DSL and the trustee responsible for online safety will be part of the online safety group.
- The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

3.2 The headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff².
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders 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.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

3.3 The designated safeguarding lead

While the responsibility for online safety is held by the DSL and cannot be delegated, the school may choose to appoint an Online Safety Lead or other relevant persons to work in support of the DSL in carrying out these responsibilities. It is recommended that the school reviews the sections below for the DSL and OSL and allocate roles depending on the structure it has chosen

- The DSL will:
 - hold the lead responsibility for online safety, within their safeguarding role.
 - Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
 - meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
 - attend relevant governing body meetings/groups
 - report regularly to headteacher/senior leadership team
 - be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all

incidents are recorded.

- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

3.4 The SLT lead for IT

- The SLT lead for IT 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
- lead the Online Safety Group
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), IT strategic lead and other staff to address any online safety issues or incidents.
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments.
- ensuring that all online safety issues are managed, logged and dealt with in line with the child protection and behaviour policies.
- have a leading role in establishing and reviewing the school online safety policies/documents
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents. Deliver online safety training to staff.
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with technical staff, pastoral staff, support staff and external agencies (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
 - content
 - contact
 - conduct
 - commerce
- Providing regular reports on online safety in school to the headteacher and/or governing board
- This list is not intended to be exhaustive.

3.5 The IT strategic lead

The IT strategic lead is responsible for:

- Ensuring that they are aware of and follow the school Online Safety Policy and IT Policy to carry out their work effectively in line with school policy
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils 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 and is not open to misuse or malicious attacks.

- Ensuring that access is blocked to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any incidents of cyber-bullying of which they are aware of are dealt with appropriately in line with the school behaviour policy.
- Ensuring that the school meets (as a minimum) the required online safety technical requirements as identified by the [DfE Meeting Digital and Technology Standards in Schools & Colleges](#).
- Ensuring that there is clear, safe, and managed control of user access to networks and devices
- Ensuring that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Ensuring that the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the online safety lead for investigation and action
- Ensuring that the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single
- Ensuring that any online safety or incidents of cyber-bullying which they are aware of are logged and dealt with appropriately in line with this policy.
- Ensuring that *monitoring systems are implemented and regularly updated as agreed in school policies*
- This list is not intended to be exhaustive.

3.6 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they follow all relevant guidance and legislation including, for example, [Keeping Children Safe in Education](#) and UK GDPR regulations
- all digital communications with learners, parents and carers and others should be on a professional level *and only carried out using official school systems and devices (where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements*
- they immediately report any suspected misuse or problem to the DSL for investigation/action, in line with the school safeguarding procedures
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are 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 lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies (n.b. the guidance contained in the [SWGfL Safe Remote Learning Resource](#))
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- Ensuring that any online safety and cyber-bullying incidents of which he is aware are logged and dealt with appropriately in line with this policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of ‘it could happen here’
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- This list is not intended to be exhaustive.

3.7 Parents

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners’ acceptable use agreement (the school will need to decide if they wish parents/carers to acknowledge these by signature)
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix)
- parents’/carers’ evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- *reinforcing the online safety messages provided to learners in school.*
- *the safe and responsible use of their children’s personal devices in the school (where this is allowed)*
- 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.

3.8 Visitors and members of the community

Visitors and members of the community who use the school’s ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

3.9 Students

Are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this should include personal devices –

where allowed)

- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should know what to do if they or someone they know feels vulnerable when using online technology.
- Should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.
- Should understand the importance of adopting good online safety 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.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. The school's curriculum for doing this will be published on the website.

5. Educating parents about online safety

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

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the SLT lead for IT.

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 one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils 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 pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

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

The school also sends information on cyber-bullying to parents so that 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 Safeguarding and Anti-bullying policies.

6.3 Examining electronic devices

Whilst investigating incidents of behavior, or supporting a student with a safeguarding concern, it is sometimes the case that a member of staff will find it helpful to see content on a student device. For example, it may be helpful for a member of staff to see screenshots linked to an issue of cyber-bullying.

In these circumstances, the following steps will be taken:

- a. The member of staff will ask the student if they may see the content. If the student refuses, the member of staff will not compel the student, but will make a DSP aware and seek guidance.
- b. If the student agrees, the member of staff will, before viewing the content, ask the student to describe what is on the screen. This is to avoid a member of staff inadvertently viewing youth produced sexual imagery.
- c. If the member of staff is in any doubt about whether they should view the content or not, they should not view the content, but immediately contact a DSP for guidance.
- d. If a member of staff views content on a student device, and judges that a copy needs to be retained in school for records, the member of staff will ask the student to take a screenshot using their device and send this to the school email address of the member of staff. This content should then be transferred to CPOMS, and the email deleted from the staff email account.
- e.

There is guidance in the Behaviour Policy about the school's protocol for conducting searches. There is also guidance in the Safeguarding Policy about youth-produced sexual imagery, and reference should be made to these policies as needed.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to confirm their acceptance of an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors.

8. Pupils using mobile devices in school

Mobile phones are not permitted to be used on the school site. There are limited exceptions to this for sixth formers, who may use mobile phones in their social and work areas and, with teacher permission, in lessons for work-related activity.

If a pupil breaches the school policy on mobile phones, the phone will be confiscated and will be held by the Headteacher in line with the school behaviour policy.

Students may bring a laptop or tablet into site, and use this with teacher permission during lesson time, and also during morning break. Full details of this are set out in the IT policy.

9. Staff using personal devices

Teaching staff are provided with school laptops, and non-teaching staff an appropriate desktop or laptop. These should be the only devices used for work purposes in school. Personal devices must not be used for schoolwork outside of school.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will take action in accordance with the principles in our Behaviour Policy.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

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, 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 pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies 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.

12. Monitoring arrangements

Online safety issues will be logged on CPOMS, in line with normal safeguarding practice.
This policy will be reviewed every year by the Assistant Head with responsibility for IT. At every review, the policy will be shared with the governing board.

Appendix 1: Student Acceptable Use Agreement

ACCEPTABLE USE AGREEMENT: STUDENTS

I understand that IT systems in school - including the internet, email, digital video and mobile technologies - are provided for educational purposes.

Learning effectively

- I will use the school IT systems to support my learning.
- I will listen carefully to the advice I am given by my teachers and use IT as they show me in order to help me learn.

Keeping safe

- I will choose a strong password. I will not reveal it to anyone. I will only log on to the school network/learning platform with my own username and password.
- If I discover an unsuitable site, I will switch the screen off and immediately tell a teacher.
- I will not bypass or attempt to bypass any of the security features provided at the school.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately
- If I feel bullied online, then I will tell my parent/ carer or a teacher.
- For school-related activities, I will only use my school email address.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone via the internet.

Showing respect for others

- I will make sure that all digital communication with students, teachers or others is responsible, appropriate, inoffensive and sensible. This is both inside and outside of school and includes use of social media.
- I will not use IT systems to bully or harass someone else.
- I will respect the privacy and ownership of others' work on-line at all times. I will not bring into school any illegal content, including pirated songs, movies, software, offensive material and will not try and share or distribute it further.
- I will seek permission from my teacher before I take, store and distribute images, audio or videos of students and/ or staff. These digital recordings must never be of an inappropriate or offensive nature. If asked to delete any digital recordings I will do so from all media (i.e. USB, home computer etc)
- I will ensure that my digital activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring it into disrepute.

Taking care of our resources

- I will not download or install software on school technologies.
- I will log off when I have finished using a computer to allow others to use the machine.
- I will not deliberately damage computer, systems or networks and will report any incidents of damage I see to staff.
- I will not consume food or drink in the IT rooms.

Use of AI

I will not use AI tools when completing NEA exam assessments.

When using AI in my work I will ensure I reference the name of the AI source and the date the content was generated.

If I use AI in my work, I will ensure I retain a copy of the question and the generated content for reference and authentication purposes in a non-editable format, e.g. a screenshot.

I will also provide a brief explanation of how AI tools have been used.

I understand that AI information may be inaccurate and that it is my responsibility to scrutinise and cross-check for its appropriateness and accuracy.

Appendix 2: Staff Acceptable Use Agreement

Digital technologies have become integral to the lives of everyone, including children and young people, both within schools and in their lives outside school. The internet and digital technologies are powerful tools, which can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. The school has the right to protect itself and its systems and all users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while online and using digital technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff are protected from potential risk in their use of technology in their everyday work.
- The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

- I understand that I must use school systems in a responsible way, to minimise the risk to the safety, privacy or security of the school community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that the school will monitor my use of school devices and digital technology systems
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of the school
- I understand that the school devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies. .
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will store my passwords securely and in line with the school's relevant security policy.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using digital technologies and systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their

express permission.

- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images, and taking account of parental permissions. I will not use my personal equipment to record these images.
- I will only use social networking sites in the school in accordance with school policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

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

- I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education / UK GDPR)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack
- When using AI systems in my professional role I will use these responsibly and:
 - will only use AI technologies approved by the school
 - will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
 - to protect personal and sensitive data, I will ensure that I do not upload sensitive school-related information into AI systems
 - will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance
- critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
- will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being

When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.

- *I will not use personal accounts on school systems.*
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will not bypass any filtering or security systems that are used to prevent access to such content.
- I will not install or attempt to install unauthorised programmes of any type on a school device, nor will I try to alter device settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Security Policy (or other relevant policy). Where

digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.

- I understand that the data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however this may have happened.
- When using the internet in my professional capacity or for school sanctioned personal use:
- I will ensure that I have appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content
- Where content is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this acceptable use agreement applies to my use of digital technologies related to my professional responsibilities, within or outside of the school.
- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.
- I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date: