E-Safety & Acceptable Use Policy

Governors Responsible:	**Jack Robson**
Nominated Lead Members of Staff:	**Headteacher / Computing & CEOP Leader**
Next Review Date:	**Autumn 2027**

Introduction:

E-safety is defined as being safe from risks to personal safety and wellbeing when using all fixed and mobile devices that allow access to the internet, as well as those that are used to communicate electronically. This includes personal computers, laptops, mobile phones, digital cameras, wearable technology (such as smartwatches) and gaming consoles such as Xbox, PlayStation and Nintendo Switch.

Safeguarding against these risks is everyone's responsibility and needs to be considered as part of the overall arrangements in place that safeguard and promote the welfare of all members of the community, particularly those that are vulnerable.

Our E-safety Policy has been written by the school, involving all stakeholders and builds on best practice and Government guidance. It relates to the latest versions of DfE statutory guidance: **Keeping Children Safe in Education** and **Generative artificial intelligence (AI) in education** as well as the **Online Safety Act 2025.** This Policy also aligns to the school's wider Safeguarding procedures and policies for all members of the school community.

Understanding the Risks and Responsibilities of Internet Use

The internet is a vital tool for learning, communication and professional development. While it offers many benefits, it also presents risks that must be managed responsibly by all members of the school community.

E-Safety encompasses not only internet use but also mobile phones and other digital communication technologies. These can be misused to harm children, including through abusive messages, inappropriate content, or online grooming. Staff have a duty of care to educate pupils about these risks and promote safe, responsible use. This policy supports a balanced approach—protecting users while encouraging exploration and learning. It serves as a guide for appropriate use of IT use both in and out of school.

As technology evolves, so do the risks. These can be grouped into three categories:

- **Content**: Inappropriate material such as violent, sexual, biased or misleading information.
- **Contact**: Unwanted interactions including bullying, harassment, grooming or data harvesting.
- **Conduct**: Unsafe behaviours such as illegal downloads, sexting, or sharing harmful content.

Much online material is intended for adults and may be unsuitable for children. Staff must remain vigilant to the risks of online grooming, where individuals may pose as peers to exploit children over time.

Cyberbullying & Cyberflashing:

Cyberbullying is bullying through the use of communication technology and can take many forms e.g. sending threatening or abusive text messages, emails or through messaging within social media websites. This bullying can be either personally or anonymously directed at individuals, making insulting comments about someone on a social networking site or blog or making/sharing derogatory or embarrassing videos of someone via mobile phone or email.

In addition, it is now a criminal offence to send unsolicited sexual images, especially of oneself, to another person's computer or phone, known as cyberflashing.

Handling Explicit Images and Online Sexual Content

In line with the latest DfE RSHE guidance (2025), Shottermill Junior School recognises the increasing risk posed by children's exposure to explicit images online including indecent content and sexting or sharing 'nudes' also known as 'Sextortion'. Staff must be vigilant in identifying and responding to incidents involving the sharing or receipt of sexually explicit material, including images or videos.

Explicit images of children are illegal and will be treated as a serious safeguarding concern.

- Pupils must be taught that creating, sharing or possessing indecent images—even of themselves—is a criminal offence under UK law.
- Staff must report any concerns immediately to the Designated Safeguarding Lead (DSL) and follow child protection procedures.
- The school will educate pupils about the risks of sexting and online exploitation through age-appropriate RSHE lessons, promoting respect, consent, and safe online behaviour.

Parents will be informed of the school's approach and supported with information to help children stay safe online when they are outside of school premises.

This aligns with the DfE's emphasis on helping children critically engage with online content, understand consent, and recognise harmful behaviours, including online misogyny and exploitation.

Why internet and digital communications are important:

Teaching and learning:

The Internet is an essential element in daily life for education, business and social interaction. We believe that the school has a duty to educate children in the safe use of technology and how this can be beneficial in modern day life. Our approach considers that children will have access to online technology within the school setting, but also in their own time at other locations. Our approach will include:

- Teaching children how to use the internet to find, search, and exchange and share information.
- Developing an understanding of new emerging technology (e.g. Artificial Intelligence) and how to use this safely and responsibly.
- Developing an awareness of filtering and monitoring of online technology and being a responsible user of technology both in and out of school. This includes key messages relating to cyberbullying and sharing our 'Stay Safe Online' poster – Appendix 1)
- The safe and effective use of the Internet in learning about the world around them, including evaluating information for bias, factual inaccuracies and negative consequences (e.g. as a means to influence or cause harm, manipulation or exploitation). This critical skill will be taught across the curriculum, not just in Computing lessons.
- Showing pupils how to use a range of software and Apps to publish and present information for a wide range of purposes to different audiences, so they are well equipped for their studies in Year 7 and beyond.
- Showing pupils how to report unpleasant Internet content and get help if ever they feel unsafe whilst accessing online content (e.g. NSPCC reporting website, 5 Trusteed adults approach)

Managing Internet Access & Roles and Responsibilities:

The school E-Safety Leader is: Mrs Jenny Zabell (CEOP Ambassador)

The designated member of the Governing Body responsible for E-Safety & Safeguarding is: Mr Jack Robson

Governors

Governors are responsible for the approval of the E-Safety policy and for reviewing the effectiveness of the policy by reviewing e-safety incidents and monitoring reports. E-Safety falls within the remit of the Governor responsible for Safeguarding. The role of the E-Safety Governor will include:

- Ensuring an E-safety policy is in place, reviewed every 2 years (or earlier if required) and is available to all stakeholders.
- Ensuring that there is an E-Safety coordinator who has been trained to a higher level of knowledge, which is relevant to the school, up to date and progressive.
- Ensuring that procedures for the safe use of IT and the Internet are in place and adhered to.
- Holding the Headteacher and staff accountable for E-Safety.

Headteacher and SLT

The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community, though the day-to-day responsibility for E-Safety will be delegated to the E-Safety Leader. Any complaint about staff misuse must be reported in line with the school's safeguarding procedures.

- Ensure access to induction and training in E-Safety practices for all users.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that staff or external providers who operate monitoring procedures be suitably trained and qualified, as well as a DBS check in place.
- Ensure that pupil or staff personal data is handled in line with GDPR policies.
- Work in partnership with the DfE, Local Authority and the Internet Service Provider, Computing Leader and school IT Technicians to ensure systems to protect students are reviewed and improved.
- Ensure the school IT system is reviewed regularly with regard to security, preventing and dealing with cyber attacks and that virus protection is installed and updated regularly.

E-Safety Leader:

The E-Safety Leader will undertake relevant training, including the CEOP training to ensure the school is aware of the key messages in relation to keeping children safe online and ways to tackle child exploitation. This will also be complemented by regular training in line with the PREVENT duty to protect children from the risks of radicalisation and extremism. Other duties include:

- Leading E-safety staff meetings and workshops for parents.
- Working in partnership with the DfE, Local Authority and the Internet Service Provider, DSLs, IT Technicians to ensure systems to protect students are reviewed and up to date.
- Receiving, investigating and reporting of E-safety incidents, filtering alerts and informing SLT so that training can be directed to preventing these issues from reoccurring.
- Liaising with the nominated member of the Governing body & Headteacher to regularly report on E-Safety and Computing.

IT Technicians:

The IT Technicians are responsible for ensuring:

- That the schools technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school has the necessary infrastructure and antivirus software in place relating to 'back up procedures', so that the school may continue to operate if a security threat occurs.
- That the school meets required E-Safety technical requirements and DfE / Government guidance that may apply.
- That unauthorised users do not gain access to the school's network through ensuring effective password and user accounts are well managed.
- That filtering systems are updated on a regular basis and routinely checked for the effectiveness.
- Stay abreast of emerging technologies (such as AI) and disseminating training to the relevant staff as required.
- They liaise with key partners such as the Local Authority, Internet Service Provider, SLT and link Governor on any matters relating to technology use in school.

Email:

- Staff may only use their approved Microsoft Outlook 365 for work related emails.
- Staff must not use school devices to check their own personal email due to the risk of opening malware.
- Staff to staff emails concerning children should use initials as identification, not full names.
- We do not routinely use email for pupils in school as other forms of communication such as Google Classroom are more appropriate for junior aged pupils.

Google Classroom or other current platforms:

- Class codes to access the classroom will only be shared between the teacher and pupils within school.
- On the occasion a child leaves the school, they will be removed from the Google Classroom.
- Comments will be monitored by the Class Teacher.
- Pupils must not reveal personal details in communications.
- Staff to pupil online communication must only take place via Google Classroom and can be viewed by SLT or parents.
- We will not respond to parent communications via Google Classroom. Instead, parents are requested to send an email to the School Office for the attention of the Class Teacher.
- Class Teachers may need to access pupils passwords to monitor/delete work and check solve log on issues.

Images or videos of children are considered to be forms of personal information:

Staff must be aware that digital photographs often contain embedded metadata (such as location, time, and device information), which can inadvertently disclose sensitive details and pose a safeguarding risk if shared publicly. For this reason, the school has decided to upload photographs of pupils' faces to Google Classroom, which is a safer and more secure platform.

Alternative pictures (e.g. photos without a pupil face) will be used on websites and social media where possible. The school recognises that they cannot fully prevent other adults from photographing children, for example at sporting or community events involving our pupils. However they will always seek to remind parents of using photographs of children responsibly and not sharing pictures without permission from another child's parent. In all cases, pupils' full names will be avoided on the school website and social media, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs or videos of pupils are used in school or published on the school website / Google Classroom / social media or in press. This will be obtained when the child joins the school to cover all uses, although a parent may withdraw or change their permission at any time.

Encrypted USB drives, memory sticks and cloud storage are a temporary means of storage for images. Once they have been used or uploaded to a secure location (e.g. the school network or Google Drive) they should be removed from the temporary storage device.

Social networking and personal details:

The school uses social media to communicate with parents and the wider community. This may include sharing positive achievements by its pupils, staff or parents or advertising school events. It is also used (where appropriate) as a means of communicating updates to parents such as when children are out on an educational visit or residential trip. The school does not respond to direct messages via social media and parents will be directed to use the school telephone number or office email address to get in touch.

In addition to this, the Parent Teacher and Friends Association have their own **PTFA Facebook Page** to directly communicate with parents. Strict codes of conduct are in place to ensure that this social networking site is monitored and managed properly. Inflammatory, negative comments about the school will be immediately dealt with by the Senior Leadership Team and in serious cases we may seek to involve the Police.

- As most social media applications and websites are for ages 13 or 16 years and upwards, the school will limit pupil access to these sites, and consider how to educate pupils in their safe use e.g. use of passwords.

- Pupils will be advised never to give out personal details of any kind, which may identify them or their location. Pupils will be advised to use nicknames and avatars when using social networking sites.

Pupils and parents will be advised that the use of social media brings a range of dangers for children such as cyberbullying or can cause health concerns in young people (e.g. loss of sleep or mental health concerns).

Managing filtering and access to inappropriate content:

Children will not be permitted to bring a mobile phone to school, or any device which has access to online or camera/videoing facilities - as they are able to bypass the school's filtering and monitoring systems. This will include any PTFA events where children are in the care of school staff (e.g. school discos). The school's rigorous approach will be widely shared in parent communications. A breach of this rule will be managed by the most senior member of staff available and will involve direct communications with the parent to ensure further instances do not occur.

- The school will work in partnership with the Local Authority to ensure systems to protect pupils meet the most recent DfE guidance.
- If staff or pupils come across unsuitable online materials, the site must be reported to a member of the Senior Leadership Team immediately, so that this can be blocked.
- SLT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Class Teachers will be responsible for overseeing the content that children access, particularly in places outside of the classroom (use of portable technologies) or at times outside of lessons (break times or after school clubs).

All staff in school should also make themselves aware of the risks posed to children by content available online. Such risks include content which may encourage or assist serious self-harm, spread dis-information or cause harm or discrimination towards others.

Use of Artificial Intelligence (AI) in School

As part of our commitment to innovation and digital literacy, Shottermill Junior School recognises the growing role of Artificial Intelligence (AI) in education. While AI tools can enhance teaching, learning, and administrative efficiency, their use must be carefully managed to ensure compliance with safeguarding, data protection, and intellectual property regulations.

Staff are expected to exercise professional judgement and seek guidance from the E-Safety Leader or Headteacher when in doubt about the use of AI technologies. Generative AI language models that are acceptable to use within the school will only include:

- **Gemini (Google) and Co-Pilot (Microsoft).**

Safeguarding Considerations:

- Staff must ensure that any AI tools used in school do not expose pupils to inappropriate content or interactions.
- AI-generated content must be reviewed before sharing with pupils to ensure it aligns with the school's values and safeguarding standards.
- Staff must not use AI tools to simulate or impersonate individuals, especially children, in any context that could compromise safety or wellbeing.
- Staff will oversee the use of AI within their teaching and must not allow children to use this directly in school.

Data Protection:

- Staff must not input personal data (including pupil names, photos, or identifiable information) into AI systems unless the tool has been approved by the school and complies with GDPR.
- AI tools must be used in accordance with the school's Data Protection Policy. Any data shared with AI platforms must be anonymised unless integrity of the system has been thoroughly checked.
- Staff must ensure that AI tools do not store or transmit sensitive data without encryption or appropriate security protocols.

Intellectual Property Rights:

- Staff must respect copyright and intellectual property laws when using AI to generate or adapt content. This includes ensuring that any AI-generated materials do not infringe on third-party rights.
- When using AI to support lesson planning or resource creation, staff must verify the originality of content and cite sources where applicable.
- AI-generated student work must be clearly identified and not misrepresented as wholly original if the AI tool contributed significantly to its creation. Pupil work will not be uploaded to AI unless the Staff are satisfied that this will not be shared widely outside of the AI model.
- The school's own work (e.g. planning, policies or ideas) will not be uploaded to AI without the express permission of the owner / SLT.

Use of Artificial Intelligence (AI) outside of School

As AI tools become more accessible, it is important that pupils aged 7–11 are guided in their safe and responsible use when completing homework or independent learning tasks. Children must be taught to use AI platforms that are age-appropriate and approved by parents or guardians. They should understand that AI-generated content may not always be accurate or suitable, and must apply critical thinking when reviewing responses.

Parents are encouraged to supervise their child's use of AI tools at home, discuss the reliability of information, and ensure that personal data is not shared. The school will seek to provide guidance to families on recommended tools and how to support children in using AI ethically and safely.

Protecting personal data:

The school is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The IT Technician will review the security of the school information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off site is encrypted
- Making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this
- Files held on the school network will be regularly checked for viruses
- The use of user logins and passwords to access the school network will be enforced
- Portable media containing school data or programmes will not be taken off-site without specific permission from the Headteacher or Deputy Headteacher. All memory sticks used must be encrypted.

For more information on data protection in school please refer to our **data protection policy**.

Data Storage and Transport:

All personal information must be kept secure. At Shottermill Junior School we employ a combination of technical and procedural solutions to maximise the security of personal data of children or adults:

- All staff laptops, chrome books and desktop computers will be password protected and staff will be encouraged to change these regularly.
- Transporting personal information off site should be avoided unless necessary.
- If personal data is required to be taken off site, it should either be stored on a password protected laptop or an encrypted memory stick and deleted when no longer needed.
- An adult should take all necessary precautions when using a school device at home to make sure that no material is accessed which could contravene any elements of this policy (e.g. this has implications for uploading personal photographs, personal use of the internet, allowing other people to use the machine, etc.)

Much of the school's planning and administrative tasks, including pupil data is stored securely within the Google Drive, which is password protected. Teachers must ensure that passwords are not disclosed to any other person to themselves. The access to Google Classroom or other current platforms will be removed once an employee leaves the school.

Only encrypted memory sticks should be used for GDPR purposes. A visitor to the school site will be prevented from using their own personal USB device on our school network, in case this introduces a virus. Instead, they will be asked to email resources or presentations in advance (e.g. for assembly).

Policy Decisions

Authorising Internet access:

1. All staff must read and sign the '**Staff Acceptable Use Agreement**' (See Appendix 2) before using any school IT resource or personal device in school.
2. The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
3. Any child who is deemed a high risk when using the Internet or any IT equipment / resource will have restricted access in school and in this exceptional circumstance, parents will be consulted on the management of IT curriculum provision offered to their child.

4. Any person not directly employed by the school will be reminded of the school's 'acceptable use of school IT resources' before being allowed to access the Internet from the school site. Use of IT resources will be monitored closely.

Assessing risks:

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will monitor IT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.
- Staff will receive regular training in emergent technologies and threats to protect service users.

Handling E-safety complaints:

- Complaints of Internet misuse will be dealt with by a member of the SLT and may be recorded on CPOMS.
- Any complaint about staff misuse must be referred to the Headteacher in line with safeguarding protocols.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Communications Policy

Introducing the E-safety policy to pupils:

- Appropriate elements of the E-safety policy will be shared with pupils.
- In all year groups, the first lesson for each half termly Computing topic will be an E-Safety lesson, tailored for the year group, using the Common Sense Education scheme.
- E-safety posters will be posted nearby to where computers or mobile devices may be used.
- Pupils will be informed and *reminded regularly* that network and Internet use will be monitored by staff and the Headteacher.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils (e.g. inviting in the Police to talk to children about personal safety).

Staff and the E-safety policy:

- All staff will be directed to read the school's E-safety Policy and its importance explained.
- All members of staff will be asked to sign the **Acceptable Use Agreement**.
- Staff will be made aware that their online use will be closely monitored and traced to the individual user and what the procedures will be for misuse of technology in line with our Staff Code of Conduct and the Capability & Disciplinary Policy.

Enlisting parents' support:

- Parents' and guardians' attention will be drawn to the School E-safety Policy in newsletters and this will be made available on the school website.
- Parents' will be directed to useful information on the school website and via email, to help them keep their children safe online.

- The school will make clear that it is the parents' responsibility to work in partnership with school to monitor their child's use of technology and ensure this does not cause behaviour of safeguarding concerns.
- Parents and carers will from time to time be provided with additional information on E-safety topics – such as parent workshops.
- In instances where the school has concerns about a child's home access to computers or online technologies including incidences of: Cyber-Bullying, meeting strangers, accessing inappropriate content such as video games above the recommended age certificate, the Child Protection Policy will be referred to and concerns dealt with in accordance with its procedures.

Appendix 1

Appendix 2:

Shottermill Junior School

Acceptable Use Agreement

Governors Responsible:	**Jack Robson**
Nominated Lead Member of Staff:	**Headteacher / IT & CEOP Leader**
Status & Review Cycle:	**Recommended (Every 2 years)**
Next Review Date:	**Autumn 2027**

Introduction

Our Acceptable Use Policy has been written by the school, involving all stakeholders and builds on best practice and Government guidance. It relates to the latest versions of DfE statutory guidance: **Keeping Children Safe in Education** and **Generative artificial intelligence (AI) in education.** This agreement should also be read in conjunction with the most recent version of the **Shottermill Junior School Staff Handbook,** which sets out the **Staff Code of Conduct**, use of electronic devices and social networking sites, safeguarding children and our expectations for upholding the highest standards of professional conduct both in and outside of the school workplace.

The aims of this policy are:

- To encourage safe use of online technologies by both children and adults working within our school.
- To encourage the development of skills to access, analyse and evaluate resources from the Internet.
- To use these resources to support teaching and learning across the curriculum.
- To ensure their supervised and appropriate use.

Guidelines:

As access can lead to any publicly available resources on the Internet, a filtered/screened service will be used in school to block access to inappropriate content or website which may pose a risk to children. All staff members will be aware of their responsibilities towards pupils, checking websites they recommend are suitable, ensuring that access is supervised and that appropriate rules are being followed.

Whenever possible, screens should always be facing the teacher. Where this is not the case the teacher must walk regularly around the group to supervise sites being accessed. Children should be aware of the problems associated with Internet access and how their actions will be monitored through staff (e.g. filtering alerts). If required, contact with the IT support team will be made to adjust filtering settings where a breach occurs.

Emails & Staff Wellbeing:

Staff may be required to use the multi-factor authentication tools App to log into their email in school, as this provides the highest level of security protection. This means that staff may be required to access their phones in classrooms. Mobile phones should only be brought out for the time that is necessary to log into emails and should be locked away thereafter.

Staff email addresses are only available for staff to use when they are working and personal emails must not be used for work related tasks. No email should be sent out to the parent or wider community without a member of SLT approving it and wherever possible, we request that you speak to a parent on the phone or face to face, rather than emailing, to avoid communications being sent to others without permission.

In order to protect the wellbeing of staff, email communications are always sent through the Office email address.

Staff are requested to avoid sending emails to other staff outside of school hours, wherever possible, to protect work/life balance. Therefore, work emails should only be sent between 7:30am and 6:00pm, Monday to Friday. Some staff may choose to work outside of these hours and so must use the 'schedule send' feature to delay sending an email to a colleague until the next working day.

Google Classroom or other current platforms:

Google Classroom is a key tool in online education. All communication with pupils must relate to the work and be minimal. We do not respond to parent comments or queries on Google Classroom, so please direct parents to email via the School Office email address instead. The use of Google Classroom will be monitored by Teachers, as well as SLT and any inappropriate comments must be reported in line with safeguarding procedures.

Virus / Malware Protection:

Cyber attacks are very real and pose a significant threat to the school's database, where we hold much personal information about children, staff and parents. The methods used by criminals are becoming increasingly sophisticated so staff must exercise the highest level of vigilance.

Virus protection is installed and kept up to date in school (current virus protection software). Computer users, especially Internet users, should be aware of the dangers of virus corruption from clicking on internet links, authorising downloads or opening attachments to emails. Staff must exercise extreme caution at all times and must never open an attachment, click on a link or respond to an email they do not recognise.

Daily virus updates and back up of the school network will be used to help prevent damage to files and systems, however the disruption caused by a cyber attack would undoubtedly be significant - therefore prevention is better than cure.

Internet and System Monitoring:

All Internet activity is monitored by the school system and checked by the school ICT technical support manager, as well as the Headteacher, Deputy Headteacher and E-Safety Leader. It is the responsibility of those designated staff to review and respond to any breaches of the school's Internet policy and/or use of obscene, racist or threatening language detected by the system.

Any serious transgressions of the school's E-Safety Policy will be dealt with in accordance with the school's Behaviour or Anti-Bullying Policy. For adults the Whistleblowing Policy and Staff Misconduct Policy may be used to follow up concerns. Concerns should be reported immediately to the Headteacher (or in the case of the Headteacher, the Chair of Governors) who will investigate and may follow up with the Local Authority Designated Officer (LADO).

Photography Publishing Statement:

The school wishes our website and social media platforms to reflect the range of activities and educational opportunities on offer at Shottermill Junior School, however, we recognise the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication, the following conditions should be adhered to:

- Wherever possible, we will not publish photographs or videos of children unless we have removed metadata and written consent of the parents/legal guardian has been obtained. Surnames of children will not be published alongside images.

- We will utilise Google Classroom as a more secure method of sharing photographs, such as from school residential visits, again with written parents/guardian permission.

- Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material may be published or not. In the case of a simple piece of artwork or writing, this may well be fine, but images of that child should not be published. If in any doubt at all, refer to the person responsible for child protection.

Staff and Volunteers must abide by the following code of conduct:

IT is seen as beneficial to all members of the School in supporting learning, teaching, research, administration and approved business activities of the School. The School's IT facilities provide a number of integral services and, therefore, any attempt to misuse a computer system could cause significant disruption to other users at the School. This could also lead to breaches of the data protection rights of a number of individuals causing harm to those individuals, and to the School.

This Acceptable Use Agreement is intended to ensure that:

- All users, will be responsible and stay safe while using IT devices, systems and services.
- School devices, systems, services and users are protected from accidental or deliberate misuse that could put the security of these systems and users at risk.

Key features of the e-safety policy will also be outlined in the **Safeguarding Leaflet for Visitors.**

Use of Artificial Intelligence (AI) – Staff Summary

Staff may use approved AI tools (Gemini by Google and Copilot by Microsoft) to support teaching and administration, provided they follow safeguarding, data protection, and intellectual property guidelines.

- AI must not be used to simulate individuals or expose pupils to inappropriate content.
- Staff must not input personal or pupil data into AI platforms unless authorised and compliant with GDPR (e.g. staff are not permitted to upload emails to generate an AI response, unless these have been anonymised and all personal information removed).
- AI-generated materials used with children must be reviewed in advance, for accuracy and originality.
- Pupil work must not be uploaded to an AI platform without parental permission and checking the system is fully secure and approved.

Staff must seek guidance from the E-Safety Leader or Headteacher if unsure about appropriate use.

Agreement

I understand that I must use School systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users, including as to the personal data of others. When using the School's technology:

- I understand that the School systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have prior permission;
- I understand that the School may monitor my use of the devices, systems, services and communications at any time;

- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it;
- I will not disclose or share personal information about myself or other service users when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details);
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online;
- I will not open any suspicious links or attachments to emails, unless I know and trust the person / organisation who sent the email, and will immediately report concerns to SLT.
- I will respect copyright and intellectual property rights by not taking, distributing, or using text, images, or other materials without permission. I will also respect others' work and files, ensuring I do not access, copy, upload, remove, or alter any content without the owner's knowledge and in accordance with school policies.
- I will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials;
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions;
- I will not use or modify any of the School devices, systems and services in any way that will disrupt their use for others in any way. I will not install or attempt to install programmes on any School device without permission, nor will I try to alter computer settings;
- I understand that I am not permitted to attempt to connect any devices or systems (e.g. laptops, mobile phones, USB devices, etc.) to any School devices, systems or services without prior permission from SLT within the School. I understand that, if I am permitted to use my own devices in the School I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- 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 policies. I will not use my personal equipment to record these images, unless I have permission from the School and from the individual to do so;
- I will not engage in any online activity that may compromise my professional responsibilities;
- I will exercise caution when posting content online (e.g. social media) —whether in a professional or personal capacity—to ensure that my actions do not bring the school into disrepute. I understand that failure to uphold these standards may result in disciplinary action in line with the Staff Disciplinary and Misconduct Policy, and/or referral to the Local Authority Designated Officer (LADO).
- I will only communicate with students, parents / carers, and other parties solely related to my employment, using official School systems. Any such communication will be professional in tone and manner;
- I recognise that a failure to comply with the policies of the School, and any misuse of IT equipment, could lead to breaches of the rights of data subjects and I will act at all times in accordance with such policies in order to avoid any inappropriate use of personal data, or the breach of the data protection rights of any individual.

I agree to follow these guidelines at all times when:

- Using or connected to the School's devices, systems and services;
- Using my own equipment inside or outside of the School in a way that is related to me being a member of this School (for example, communicating with other staff, accessing School email, websites and services).

I have read and understand that use of the School IT systems and devices is governed by the full Acceptable Use Policy. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the organisation's most recent Acceptable Use Policy.

User Signature:

Full Name …….... (print) Signature ……

Date …… Job title ……..