Cheshire Academies Trust

Inspiring hearts and minds

Online Safety Policy

Hebden Green School

Next Update: Autumn 2026

Scope of this policy:

This policy applies to all members of Hebden Green School staff, pupils, volunteers, parents/carers, visitors, community users) who have access to or use the school's digital technology, systems, networks, internet access or digital communication tools, both on and off site.
It sets out how the school will:

- Protect pupils from online harm in line with the 4Cs (Content, Contact, Conduct, Commerce) as outlined in KCSiE 2025.
- Embed online safety education within the curriculum.
- Ensure that technical systems (filtering and monitoring) are effective and proportionate.
- Support staff, parents and pupils to build digital resilience.

Policy Aims

- To safeguard pupils from inappropriate online content, harmful contact, unsafe conduct, and exploitative commerce.
- To educate pupils to use technology safely, responsibly, and respectfully.
- To support staff and parents to understand online risks and their role in promoting safe use.
- To ensure robust systems of reporting, response, and record-keeping in relation to online safety incidents.
- To ensure compliance with safeguarding duties in KCSiE 2025, the Prevent Duty, Data Protection Act 2018, and UK GDPR

Schedule for Development/Monitoring/Review

- The implementation of this Online Safety policy will be monitored by the Headteacher, Deputy Headteacher, Senior Leadership Team and Online Safety Lead
- Monitoring will take place at least once per annum
- The Local Governing Board will receive a report on the implementation of the Online Safety Policy generated by the monitoring group at least once per annum:
- The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.
- Should serious online safety incidents take place, the following external persons / agencies should be informed:
    - Steve Ellis – CEO, CAT
    - Luci Jones – Director of Operations
    - Chair of Governors
    - CAT IT Support – SevenEleven Systems
    - Police (if required)
    - Local Safeguarding Teams (if required)

Hebden Green will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys & questionnaires of pupils/parents/staff
- Audit activity as required throughout the year to prevent, as well as in response to any online safety incidents arising.

Roles and Responsibilities

Local Governing Body

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents

and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor in line with their role as Safeguarding Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator / Officer
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- updates and reporting to relevant Governors / Board / Committee / meetings.

Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, although the day to day responsibility for online safety will be delegated to the Online Safety Lead.

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 staff. This process can be found in flow chart form in the appendix.

The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher and 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. These systems will include:

- Up to date acceptable usage agreements for all pupils within Hebden Green (where appropriate)
- Up to date acceptable usage agreements for all staff and volunteers at Hebden Green
- Central records of reports of misuse of technology within Hebden Green, including reports, investigations and outcomes,
- Central records of monitoring logs of online safety incidents and appropriate action(s) arising from such incidents.
- Central records of staff training given in relation to matters of Online Safety.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Officer.

Online Safety Lead

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / MAT / relevant body
- liaises with school technical staff (linked to online safety)
- receives reports of online safety incidents and creates a log of incidents to inform future online safety development
- meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors / Directors
- reports regularly to Senior Leadership Team

Network Manager/Technical Support

Hebden Green Schoo receives technical support through a formal service level agreement with SevenEleven Systems.

They are responsible for ensuring:

- the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- the academy meets required online safety technical requirements and any Local Authority / MAT / other relevant body Online Safety Policy / Guidance that may apply,
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed,

- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person,
- 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,
- the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leaders; Online Safety Lead for investigation / action / sanction,
- that monitoring software / systems are implemented and updated as agreed in academy policies.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current academy Online Safety Policy and practices,
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP) (See appendix 1)
- they report any suspected misuse or problem to the Principal / Senior Leader; Online Safety Officer for investigation / action / sanction,
- all digital communications with students / pupils / parents / carers 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 activities,
- students / pupils understand and follow the Online Safety Policy and acceptable use policies,
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead

Will be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding 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

Pupils (where applicable)

- are responsible for using the academy digital technology systems in accordance with the Pupil Acceptable Use Agreement
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's Online Safety Policy covers their actions out of school, if related to their membership of the school as covered within the Home School Agreement.

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platforms and information about national/local online safety campaigns/literature.

Parents and carers will be encouraged to support the academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line student/pupil records
- their children's personal devices in the academy (where this is allowed)

Community Users

Where applicable, Community Users who access academy systems/website/Learning Platform as part of the wider academy provision will be expected to sign a Community User AUA before being provided with access to academy systems.

Online Safety Education

Pupils (where applicable)

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

Online safety will be a focus across all areas of the curriculum, specific to age, phase, pathway and individual need. This will be embedded within the curriculum and can be can be found within curriculum planning (lead: Danielle Lamb)

Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, particularly within the ever changing technological age we find ourselves in. However, they play an essential role in the education of their children and in the monitoring/regulation of their children's online behaviours.

Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Hebden Green School will therefore seek to provide information and awareness to parents and carers (where appropriate) through:

- Curriculum activities
- Letters, newsletters, website
- Parent/carer evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to relevant web sites, publications and support materials.

Staff/Governors

It is essential that all staff, governors and volunteers receive regular online safety training and understand their responsibilities, as outlined in this policy. Training is a vital part of ensuring that the whole school community is confident in supporting children to stay safe online.

Training will be provided in the following ways:

- **Annual training**: All staff receive safeguarding and online safety training every year, with additional updates during the year as required (e.g. to reflect new risks, statutory updates or local incidents).
- **Induction**: All new staff, governors and volunteers complete online safety/Cyber Security training as part of their induction before being given access to school systems. This ensures they fully understand the school's Online Safety Policy and Acceptable Use Agreements.
- **Governors**: Governors receive updates on online safety as part of their safeguarding responsibilities, including how to interpret filtering and monitoring reports.
- **Training needs audit**: The school will carry out regular audits of training needs. Central records of training will be kept on staff files and in the Online Safety Training Log

- **Performance development**: Where online safety is identified as a training need during performance development discussions, appropriate training and support will be provided by the Online Safety Lead or external providers.
- **Policy updates**: The Online Safety Policy and any updates will be shared and discussed at staff meetings, INSET days and team briefings to ensure consistent understanding.
- **Ongoing guidance**: The Online Safety Lead (or nominated person) will provide targeted advice, guidance and training to individuals as required.

This programme ensures that staff, governors and volunteers are confident in their role, aware of current and emerging online risks (including AI, misinformation and online scams), and able to promote safe, responsible and effective use of technology across the school community.

Safer Use of Technology

Hebden Green School uses a wide range of technology to support learning, communication and administration. This includes:

- Computers, laptops, iPads, tablets and other digital devices
- The internet, including search engines and educational websites
- Email systems
- Games-based and interactive learning technologies
- Digital cameras, webcams and video recorders

All school-owned devices will be used in accordance with our Acceptable Use Policies and with appropriate safety and security measures in place.
To promote safe and effective use of technology:

- Members of staff will always evaluate websites, tools and apps before use in the classroom or when recommending them for home learning.
- The use of internet-derived materials by staff and learners must comply with copyright law, with all sources acknowledged.
- Supervision of learners will always be appropriate to their age and ability.

Filtering and Monitoring

The Headteacher and Online Safety Lead will review the effectiveness of filtering and monitoring systems at least annually, ensuring they are appropriate, proportionate, and do not over-block educational content.

- Hebden Green school Smoothwall Monitoring filtering and monitoring systems.
- Filtering is reviewed regularly and is designed to meet statutory requirements, including protecting pupils from extremist and terrorist content.
- Logs are checked by the DSL/Online Safety Lead and reported to governors where appropriate.
  Devices
- School-owned devices are provided for educational use only.
- Staff must not use personal devices to photograph or communicate with pupils.

Visitors

- Visitors are required to follow safeguarding guidance and Acceptable Use terms.
- Where access is permitted (e.g. for contractors), this will be monitored and restricted to the purpose of their visit.

Images

- Parent/carer consent must be obtained before publishing any pupil images.
- Pupil names will not be published alongside images.
- Images must only be captured and stored using school-owned devices, in line with safeguarding expectations.

Data Protection and Security

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR) announced in 2016. How Hebden Green conforms to the updated requirements of the above legislation, as well as how this supports this Online Safety Policy can be found within the Trust Data Protection Policy.

Hebden Green School is responsible for ensuring that its IT systems, infrastructure and network are as safe and secure as reasonably possible and that policies and procedures within this policy are fully implemented.

Access and Permissions

- Access to data is role-based: staff are only given access to the systems and files necessary for their work.
- Protected files and sensitive data are hidden from unauthorised users.
- Staff are not automatically granted access to the full management information system.

Passwords and Devices

- All users must use strong passwords and never share them.
- Devices that access school systems must be password-protected, locked when unattended and set to auto-lock after a short period of inactivity.
- Personal data must only be accessed on secure, school-managed devices. Private equipment must not be used to store or access personal data.

Storage of Data

- Portable media (e.g. USB sticks) should only be used where absolutely necessary, and must always be encrypted and password protected.
- The preferred method of storing and sharing data is through the school's secure, cloud-based system (OneDrive), which provides encrypted services as standard.
- Staff must not share usernames or passwords. Where documents are shared, this must be done through the OneDrive sharing facility.

Secure Transfer and Remote Access

- Personal or sensitive data may only be removed from the school premises with the permission of the Headteacher and must always be encrypted, password protected and transported securely.
- Staff must ensure that personal devices or home computers are never used to access or store school personal data.
- Where school data is accessed remotely, secure login procedures must be used.
- All portable and mobile devices used to transmit or store school information must use approved encryption and security software.

Failure to follow these rules may result in disciplinary action in line with the Staff Code of Conduct. Serious breaches may be treated as a safeguarding or data protection incident and reported to the relevant authorities.

Social Media and Communications

Clear, professional and safe communication between staff, pupils and parents is vital to support learning and to safeguard the whole school community. At Hebden Green School, all communication must comply with safeguarding, confidentiality, data protection and acceptable use policies.

Communication

- Staff must only use official school communication systems (e.g. school email, approved learning platforms) when contacting pupils, parents or carers. Personal email, text messaging, or social media must not be used.

- All email and digital communications are monitored. Staff should therefore ensure tone and content are always professional.
- Any communication that makes a staff member feel uncomfortable, or is offensive, discriminatory, threatening or bullying in nature, must be reported immediately to the DSL/Online Safety Lead.
- Pupils are taught about safe and respectful communication online, including the risks of sharing personal details and strategies for dealing with inappropriate contact.
- Sensitive information must never be shared via unsecured channels. Where necessary, approved secure systems (e.g. encrypted email) must be used.
- Personal information about pupils, parents or staff must not be posted on the school website or shared outside secure school systems.

Staff Use of Social Media

Staff must maintain clear professional boundaries online. To protect both staff and the school, staff must not:

- Refer to pupils, parents or colleagues on personal social media accounts.
- Engage in online discussions about school-related matters on personal platforms.
- Attribute personal opinions to the school or the trust.
- Connect with current or past pupils, or parents, on social media (except where a prior personal relationship exists).
- Post, like, comment on, or share material that could be deemed offensive, discriminatory, inflammatory or damaging to the reputation of the school.

Staff should regularly check privacy and security settings on personal accounts to minimise the risk of personal information being shared inappropriately. Breaches of this guidance will be managed under the Staff Code of Conduct.

School Use of Social Media

Hebden Green School maintains official social media accounts to share information with the wider community. These are managed in line with safeguarding expectations and overseen by the Headteacher and Online Safety Lead. The school ensures that:

- Accounts are checked regularly to ensure compliance with school policies.
- Communication via social media is one-way, with comments and interactions restricted where possible.
- Followers, comments, likes and other interactions are monitored and, where necessary, removed.
- At least two members of staff (including the Headteacher) are involved in the administration of school social media accounts.
- Clear systems are in place for reporting and addressing misuse or abuse of school social media platforms.

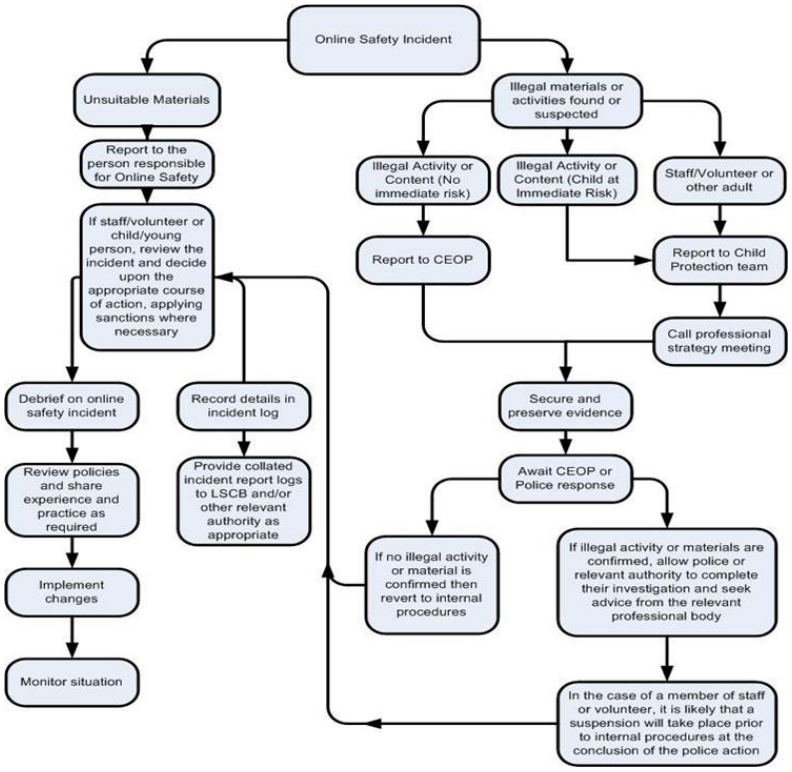
Reporting and Responding to Incidents

This guidance is for all staff when reporting or managing incidents involving the use of online services or technology. It promotes a safe and secure approach to incident management.
Online safety incidents may involve illegal or inappropriate activities, but may also arise from mistakes or misjudgements by otherwise well-intentioned users. All incidents must be taken seriously and handled in line with school safeguarding procedures.

- **Immediate action**: If there is any suspicion that a website, platform or device may contain child abuse images, or if there is any other suspected illegal activity, this must be reported to the DSL immediately and referred to the police. (See flowchart below).
- **Reporting process**: All concerns, whether involving staff, pupils, parents or visitors, must be reported promptly to the DSL (or deputy). Incidents will be logged and acted upon in accordance with safeguarding procedures.
- **Illegal activity**: Any suspected criminal activity or illegal material will be referred without delay to the police and relevant external agencies.
- **Child-centred approach**: Pupils are encouraged to follow the "Stop, Block, Report" message and to seek help from a trusted adult whenever they encounter something online that worries them.

- **Support**: Staff will ensure that any child affected by an online safety incident receives appropriate support and guidance. Where necessary, parents/carers will be informed and external agencies engaged.

This structured approach ensures that all online safety incidents are managed consistently, proportionately and with the protection of children at the centre.



Sanctions

At Hebden Green School, most online safety incidents are expected to involve inappropriate rather than illegal misuse of technology. It is important that such incidents are addressed quickly, proportionately and consistently, so that members of the school community understand expectations and trust that concerns are dealt with.

- **Proportionate response**: All incidents of deliberate misuse of technology, in breach of this Online Safety Policy or associated Acceptable Use Agreements, will be addressed in line with the school's Behaviour Policy (for pupils) or Staff Code of Conduct (for staff).
- **Escalation**: Repeated or serious misuse may result in restricted access to technology, parental involvement, formal disciplinary action, or referral to external agencies where necessary.
- **Transparency**: Where appropriate, staff and pupils will be made aware that incidents have been dealt with, to reinforce understanding of safe and responsible behaviour.
- **Illegal misuse**: Where misuse involves illegal activity, this will be treated as a safeguarding or criminal matter and referred to the police or relevant authorities immediately.

This approach ensures that online safety breaches are managed fairly and consistently, while emphasising education, responsibility, and safeguarding.

Technical – Infrastructure, Filtering and Monitoring

Hebden Green School will be responsible for ensuring that the academy infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people with responsibility sections will be effective in carrying out their online safety responsibilities. Whilst the academy has an overall responsibility to ensure the following criteria are met, it will work with Seven Eleven Systems to ensure:

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements,
- There will be regular reviews and audits of the safety and security of academy technical systems,
- All users will have clearly defined access rights to academy technical systems and devices.
- The "master / administrator" passwords for the academy ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg academy safe).
- Office staff are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. Where changes to filters are requested, they are logged and kept on central record with reasons why the change was requested and the merit it held.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Academy technical staff regularly monitor and record the activity of users on the academy technical systems and users are made aware of this in the Acceptable Use Agreement (see Appendices).
- An appropriate system is in place (by reporting to the Online Safety Lead) for users to report any actual / potential technical incident / security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- In the event that any personal device is allowed to be connected to the academy network, users abide by the acceptable usage policy and the terms detailed within it.

Staff Use of Personal Devices and Mobile Phones

At Hebden Green School, staff must use personal devices in line with the law and school policies on confidentiality, safeguarding, data security and acceptable use.

Staff must:

- Keep personal devices stored securely (e.g. locked drawer/locker) and switched off or on silent during lessons.
- Avoid using personal devices during teaching, unless authorised by the Headteacher in exceptional circumstances.
- Only bring content onto site that is appropriate and consistent with their professional role.
- Never use personal devices to contact pupils or parents/carers. Any pre-existing relationships that may affect this rule must be discussed with the DSL (or deputy) and/or Headteacher.
- Never use personal devices to take or store photographs or videos of pupils; only school-provided equipment may be used for this purpose.
-

Any breach of these expectations will be managed under the Staff Code of Conduct and Allegations Policy. Where there is reason to believe illegal content is stored or a criminal offence has been committed, the police will be contacted.

Visitor's Use of Personal Devices

At Bexton Primary School, the safety and privacy of pupils is paramount. Parents, carers, volunteers and contractors must follow school safeguarding rules on personal device use.

- Visitors should not use personal devices on the premises unless it is essential for the purpose of their visit.
- Leaders may request devices are left securely at the school office for safekeeping during the visit.
- Safeguarding notices, signage and information will remind visitors of these expectations.
- Visitors on site regularly or for extended periods must follow the school's Acceptable Use Policy and associated safeguarding policies.
- Staff are expected to challenge any inappropriate use of personal devices by visitors and report concerns immediately to the Headteacher/DSL (or deputy).

Appendix

Appendix 1 – Staff AUP

EXAMPLE: Staff and Volunteer Acceptable Use Agreement

Staff / Volunteer Name:

Signed:

Date:

Purpose
Digital technologies are integral to education and professional life. They support learning, creativity, communication, and school operations. With these opportunities come responsibilities: all staff and volunteers must use technology safely, lawfully and professionally to protect themselves, pupils, colleagues and Hebden Green School.

This Acceptable Use Agreement ensures that:

- Staff and volunteers act as responsible users who safeguard themselves and others.
- School systems and data are protected from misuse or security risks.
- Staff are clear about professional boundaries when using technology.

Agreement

Professional and Personal Safety

- I understand the school monitors my use of digital technology and communications systems.
- I will use school systems primarily for educational purposes. Limited personal use may be permitted in line with school policy.
- I will keep my username and password secure and never share them.
- I will immediately report illegal, inappropriate or harmful content or incidents to the DSL or Headteacher.

Professional Conduct Online

- I will communicate professionally at all times, avoiding offensive or inappropriate language.
- I will not access, copy or alter other users' files without permission.
- I will only take and publish images in line with school policy, using school equipment (not personal devices) and with appropriate consent.
- I will only communicate with pupils and parents/carers through official school systems.
- I will not engage in online activity that compromises my professional role.

Use of Devices and Data

- When using mobile devices or personal equipment in school, I will follow the same rules as for school-owned devices. Devices must be secure, virus-protected and password-protected.
- I will not use personal email accounts for school business.
- I will not install unauthorised software or attempt to bypass school security systems.
- I will not access or download illegal or harmful materials.
- I will handle personal data securely and in line with school policy, ensuring digital data is encrypted and paper records are stored safely.
- I will report any equipment faults or damage immediately.

Copyright and Fair Use

- I will respect copyright and only use original work of others with permission.
- I will not distribute copyrighted material without authorisation.

Responsibilities Beyond School

- This agreement applies to my use of school systems both in and out of school, and to my use of personal devices in any school-related context.
- I understand that breaches may result in disciplinary action, which could include warnings, suspension, referral to the governing body, or police involvement if illegal activity is suspected.

Declaration
I have read and understood this agreement. I agree to use school digital systems (in and out of school) and any personal devices used for school purposes responsibly, safely, and in line with this policy.