Emmbrook Junior School

Online Safety Policy

Responsibility of: Pupil Outcomes, Parental, Communication and Curriculum (POPC) Committee
Date of Policy: May 2019
Date of Review: Jan 2022
Next Review: Jan 2024

Mission Statement

We provide an inclusive, positive environment in which we nurture and empower our children to develop life-long learning skills. This enables them to grow into reflective, successful and well-rounded individuals in our global community.

Roles and Responsibilities

1.1 Governors

Online safety falls within the remit of the Safeguarding Governors and as such, Governors are responsible for the approval of the Online Safety Policy (including Acceptable Use Agreements), ensuring that it is implemented and reviewing its effectiveness.

Governors may require/undertake the following regular activities:

- Meetings with the member of staff responsible for online safety.
- Monitoring of online safety incident logs.
- Reporting to relevant governor committees.
- Keeping up to date with school online safety matters.

1.2 Head Teacher

The Head Teacher is responsible for ensuring the overall safety, including online safety, of members of the school community. The Designated Safeguarding Lead (DSL) holds a responsibility for online safety as part of their role (as noted in the 2018 Keeping Children Safe in Education statutory guidance). On a practical day to day basis, others may have particular duties relating to Online Safety, e.g. the Computing Subject Leader. However, the Head Teacher will ensure the following:

- Staff with online safety responsibilities receive suitable and regular training enabling them to carry out their online safety roles and to train other colleagues as necessary.
- The Senior Leadership Team (SLT) receives regular monitoring reports.
- There is a clear procedure to be followed in the event of a serious online safety allegation being made against a member of staff.

1.3 Online Safety Co-ordinator (Computing Subject Leader)

As noted above, the Designated Safeguarding Lead holds a responsibility for online safety as part of their role (as noted in the 2018 Keeping Children Safe in Education statutory guidance). The Online Safety Co-ordinator may in turn work with others (e.g. Network Manager/Technician) to ensure that policies are put into practice. The specific duties of an Online Safety Co-ordinator would need to be confirmed in conjunction with the DSL to ensure absolute clarity about responsibilities, but might include:

- Take a leading role in establishing and reviewing the school's Online Safety Policy and associated documents.
- Provide training and advice for staff and ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provide materials and advice for integrating online safety within schemes of work and check that online safety is taught on a regular basis.
- Liaise with the school's Designated Safeguarding Lead.
- Liaise with the school's IT technical staff.
- Ensure that online safety incidents are reported and logged (via CPOMs) and used to inform future online safety developments.
- Report to the governors and meet with them as required.
- Report regularly to the SLT.

1.4 IT Support Provider

The IT Support Provider will be responsible for ensuring that all reasonable measures have been taken to protect the school's network(s). This will involve ensuring the following:

- The IT infrastructure is secure and protected from misuse or malicious attack.
- The school meets the online safety technical requirements outlined in any relevant online guidance.
- Users may only access the school's network(s) through a properly enforced password protection policy.
- The school's filtering policy is applied and updated as appropriate.
- Any inappropriate use of the school's computer systems will be reported to the appropriate senior person.
- Provide secure external access to the school network as appropriate.

1.5 Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They are familiar with current online safety matters and the school's Online Safety Policy and practices.
- They have read and understood the school's Staff Acceptable Use Policy (AUP) and signed to indicate agreement.
- They report any suspected misuse or problem to the Online Safety Co-ordinator for investigation and action.
- Electronic communications with pupils will be on a professional level and only carried out using approved school IT systems.
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school's Online Safety and Acceptable Use Policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations in relation to their age.
- They monitor IT activity in lessons, extra-curricular and extended school activities.
- They are aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement school policies with regard to these devices.
- They know and follow the procedure for dealing with any unsuitable material that is found in internet searches.

1.6 Designated Safeguarding Lead (DSL)

The DSL holds the responsibility for online safety as part of their role (as noted in the 2018 Keeping Children Safe in Education statutory guidance). They will be trained in online safety issues and be aware of child protection matters that may arise from any of the following:

- Sharing or loss of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyberbullying

1.7 Data Protection Officer (DPO)

The DPO has a related role which is detailed in Data Protection policies and related documentation.

2 Reviewing, Reporting and Sanctions

2.1 Review

- This policy will be reviewed and updated annually.
- The school will audit provision to establish if the Online Safety Policy is adequate and that its implementation is effective.

2.2 Acceptable Use Agreements

- All users of school IT equipment will sign the appropriate Acceptable Use Agreement. This includes all staff and pupils.
- Parents may be asked to sign on behalf of their children or to show agreement with and support for the school's policy.

  [See *'Appendix 3 – Exemplar Acceptable Use Agreements'* for further information]

2.3 Reporting and logging

- The school will produce clear guidelines as to what should be done if inappropriate content is found when accessing the internet.
- Any such occurrence will be logged for review and any necessary actions that arise.
- All pupils and teachers should be aware of these guidelines.

  [See *'Appendix 1 – Course of action if inappropriate content is found'* for further information]

2.4 Complaints regarding internet use

- Any complaints relating to internet misuse should be made in accordance with the school's existing complaints procedure.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

2.5 Sanctions

- Failure to comply with the requirements of this policy will be dealt in line with the school's existing policies on behaviour, rewards and sanctions.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 or other related legislation. This would constitute a disciplinary matter in the case of staff.

3 Communications & Communication Technologies

3.1 Mobile phones and personal handheld devices

- Pupils will not be allowed to bring mobile phones to school unless prior arrangements are made with the school in which case an agreement form must be completed by parents/carers prior to phones coming into school.
- Where it is agreed mobile phones are allowed in school they must be handed in so they can be stored centrally by the Admin team. Phones will remain off until children are off school premises.
- Pupils will not be allowed to bring in games devices, particularly those which allow ad hoc networks to be established.

- Teacher/parent contact will normally be by the main school telephone and not via a mobile device except where off-site activities dictate the use of a mobile phone and this has been agreed with the school.
- Parent helpers in school and staff must ensure that they do not send personal messages, either audio or text, during contact time with pupils. If an exceptional emergency arises they will arrange temporary cover whilst they make a call.
- Staff and pupils may send educational messages during lesson times using school devices e.g. laptops, tablets if these are part of the curriculum. Personal devices will not be used for this purpose.
- Staff, helper and visitor mobile devices will normally be switched off or to silent mode during the times that children are present.
- No device in any school building should contain any content that is inappropriate or illegal.

3.2 E-mail and messaging

- Pupils and staff will be informed that the use of school e-mail or messaging accounts may be monitored.
- Pupils should report any receipt of an offensive e-mail or message on school IT systems.
- Pupils should not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an e-mail or message.
- Information of a sensitive nature should not be sent by unencrypted e-mail.

3.3 Social networking

For the purpose of this policy social networking is considered to be any digital media or medium that facilitates interaction.

- Staff use of social networking should be compatible with their professional role and show the highest standards of integrity.
- Pupil use of social networking should conform to age restrictions.

  [See *'Appendix 2 – Social Networking Guidance'* for further information]

3.4 Internet usage

- Pupils and staff will be informed that internet access will be monitored.
- The school will take all reasonable precautions to ensure that users access only appropriate material. Whilst it is not possible to guarantee that unsuitable material will never appear on a school computer the school will take appropriate measures to prevent a reoccurrence, including contacting the service provider.
- Users must not create, download, upload, display or access knowingly, sites that contain pornography or other unsuitable material that might be deemed illegal, obscene or offensive.
- Unauthorised users must not attempt to disable, bypass or reconfigure any filtering, virus protection or similar.
- All pupils using the internet, and associated communication technologies, will be made aware of the school's online safety guidelines. These will be posted near to the computer systems.
- Pupils will receive guidance in responsible and safe use on a regular basis

3.5 Digital and video images

Parental permission

- The school will ensure that, where appropriate, consent is obtained for the taking and use of digital and video images of pupils. Such use could include the school website or social media; display material in and around the school or off site; the school prospectus or other printed promotional material; local/national press.
- Pupils will not be identified by name in any title or commentary accompanying digital or video images that is in the public domain, unless specific parental consent has been obtained.
- Where parental permission has not been obtained, or it is known that a pupil should not be photographed or filmed, every reasonable effort will be made to ensure that a pupil's image is not recorded.

Storage and deletion

- Images should be uploaded to a secure location that is the control of the school. Where memory cards, USB drives, CDs or cloud storage are used during the process of capture or transfer, users should ensure that these are deleted and cleared from any temporary storage or recycle bins.
- Images should be deleted in line with the school's procedures on data retention and disposal.

Recording of images

- School digital devices should always be used to record images of pupils (subject to any variation the school agrees as noted below in 'Use of staff personal devices').
- All pupils appearing in images should be appropriately dressed.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- All digital devices capable of taking photographs and recording sound or video, whether belonging to the school or personal, may be subject to scrutiny if required.
- Where volunteers are supporting school staff, they should abide by the same rules as school staff.

Use of staff personal devices

It is recognised that the most straightforward approach is not to allow use of personally owned devices (e.g. staff smartphones, personally owned cameras) to record children. Where the situation requires variation from this, e.g. for off-site activities, the following should apply:

- It will be clearly understood under what circumstances it is permissible to use a personal device and agreed with a member of SLT in advance.
- Images will be transferred to a secure location on the school's system as soon as possible and the originals/any copies fully deleted.
- Such staff personal devices should be passcode protected.

Parents taking photographs or video

Where the school chooses to allow the recording of images at 'public' events the following should apply:

- Images may only be recorded for personal use and can only be shared with family and friends. They must not be shared on social networking sites or other websites that are accessible by the general public.

Events/Activities involving multiple schools

- When taking part in events organised by other schools or organisations, e.g. sports or music events, the schools involved will consider what image guidelines should apply.
- For larger events it is reasonable to expect that specific image guidelines should be in place. Where relevant these should include reference to press images.
- Consideration should be given as to how those attending the event will be informed of the image guidelines that apply, e.g. a letter before the event, announcement at the event, or information in any printed programme.
- Although the school will make reasonable efforts to safeguard the digital images of pupils, parents should be made aware that at some types of event it is not always realistic to strictly enforce image guidelines. The school cannot therefore be held accountable for the use of images taken by parents or members of the public at events.

4 Infrastructure and Security

4.1 Security

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that procedures outlined within this policy are implemented by those responsible.

- School IT technical staff may monitor and record the activity of users on the school IT systems and users will be made aware of this.
- Servers, and communications cabinets should be securely located and physical access restricted.
- Wireless systems should be appropriately secured.
- All users will have clearly defined access rights to school IT systems.
- Access to the school IT systems will cease when a pupil leaves or, in the case of a member of staff, ceases to be employed by the school.
- Appropriate procedures should be in place for secure storage and access to 'Administrator' passwords.

4.2 Passwords

All staff are provided with an individual password. Pupils will have an individual password for accessing the network where possible, though a group password may be acceptable for young children.

Schools should advise staff on the choice and use of passwords. The following areas may also be appropriate:

- 'Strong' passwords should be used.
- No individual should tell another individual their password.
- No individual should log on using another individual's password, unless they are a member of staff logging on as a pupil for sound educational or technical reasons.
- Once a computer has been used, users must remember to log off.
- Users leaving a computer temporarily should lock the screen (Windows key + L on a PC).

4.3 Filtering

The school maintains and supports the managed filtering service provided by NetSweeper, the Internet Service Provider (ISP).

- Changes to network filtering should be approved by the appropriate person(s).
- Any filtering issues should be reported immediately to the ISP.

4.4 Virus protection

- All computer systems, including staff laptops/devices, should be protected by an antivirus product which is preferably administered centrally and automatically updated.

4.5 Staff laptops/devices and flash drives

Where staff laptops/devices and flash drives are to be taken out of school, it is possible that they may contain sensitive data, therefore the schools should ensure that all such devices and removable media are encrypted.

The following security measures should also be taken with staff laptop/mobile devices:

- Laptops/devices must be out of view and preferably locked away overnight whether at school or home.
- Laptops/devices should not be used for purposes beyond that associated with the work of the school, e.g. by the family of a member of staff.

- Where others are to use the laptop, they should log on as a separate user without administrator privileges.

  [See *'Appendix 3 – Exemplar Acceptable Use Agreements'* for further information]

4.6 Data protection

See Data Protection Policy for specific guidance in relation to the security of personal data.

5 Online Safety Education

5.1 Learning and teaching for pupils

- Pupils should be encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school.
- Pupils should be helped to understand the need for an Acceptable Use Policy and, depending on age, asked to sign to indicate agreement.
- Pupils should be taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Key online safety messages will be included within the curriculum and reinforced as part of a planned programme of assemblies and other appropriate opportunities.
- Rules for the use of computers/devices should be displayed in all rooms and displayed next to fixed site computers.

5.2 Staff training

- Staff will be kept up to date through regular online safety training.
- Staff should always act as good role models in their use of IT, the internet and mobile devices.

5.3 Parental support

The support of, and partnership with, parents will be encouraged. This is likely to include the following:

- Awareness of the school's policies regarding online safety and internet use; and where appropriate being asked to sign to indicate agreement.
- Practical demonstrations and training
- Advice and guidance on areas such as:
  - filtering systems
  - educational and leisure activities
  - suggestions for safe internet use at home

5.4 Remote Learning Safety Guidelines

Emmbrook Junior School will record all live sessions and these will be stored securely within Teams. This is so that should any issues were to arise, the video can be reviewed. If parents of children at home do not consent to this, they have the right to decline the session invitation or limit their child's participation to 'audio only' (so the video option is turned off).

Teaching staff will share their screen during lessons to allow children at home to access the lesson remotely. No child in school will be visible on screen although their voices may be heard.

Any 1:1 sessions will only take place with the parents' permission and an adult at home is encouraged to be within earshot.

All children participating in remote learning from home must be appropriately dresses, as should anyone else in the household.

Any electronic devices used to access remote learning should be positioned in view of an appropriate backdrop, and where possible be against a neutral or blurred background.

No contact between other members of the household and children in the session (other than the child in their household) is permitted.

Live sessions will be started promptly according to the scheduled time.

Language used in live sessions must be appropriate, including any family members in the background.

Should you feel concerned about the content of the session or a situation that has occurred during it, contact the class teacher or Deputy Head Teacher immediately to report it.

Expectations for remote learning:

Please make sure that your child is seated somewhere quiet where they can hear the audio and see the screen.

Children should log in promptly to each learning session so that they do not miss key information.

If your child is unable to attend a session, they can access the recording in Teams at a later point.

Ensure your child is dressed appropriately as they will potentially be seen by a number of other children and school staff.

If you do not want your child's image to be seen on screen, please turn your web cam off or cover the camera for the duration of the meeting. (We respect your decision on this.)

If the member of staff hosting the meeting raises their hand with a flat palm, all children in the meeting must be quiet - this is a learning opportunity and therefore we will follow the school procedures as best we can during this time. It is within the rights of the teacher to 'mute' the session should noise be distracting to the session.

Adults at home – we ask that you do not participate in any school-based meetings unless you have been specifically invited to. If you have any questions about the session, please email the teacher using the Year group email address.

Apart from the school, no child or adult is permitted to record, capture or photograph the screen during a school-based meeting. This is to ensure that we adhere to confidentiality and safeguarding procedures.

Any recordings of sessions accessed for the purpose of remote learning are not to be shared in any forum and remain the property of Emmbrook Junior School.

Do not share the meeting links with anyone else.

Children are not to 'share their screen' unless instructed to do so by the teacher in charge of the session.

Teachers have a right to end sessions/individual participants if they do not follow the code of conduct.

Appendix 1 – Course of action if inappropriate content is found

- If inappropriate web content is found (i.e. that is pornographic, violent, sexist, racist or horrific) the user should:
    - Turn off the monitor or minimise the window.
    - Report the incident to the teacher or responsible adult.
- The teacher/responsible adult should:
    - Ensure the well-being of the pupil.
    - Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the pupils).
    - Report the details of the incident to the Online Safety Co-ordinator.
- The Designated Safeguarding Lead, Online Safety Co-ordinator or other appropriate person will then:
    - Log the incident and take any appropriate action.
    - Where necessary report the incident to the Internet Service Provider (ISP) so that additional actions can be taken.

Appendix 2 – Social networking guidelines

Staff conduct

- Staff will always conduct themselves with the highest standards of professional integrity and be aware that how they as individuals are perceived in the virtual world may reflect on how the school is perceived.
- Staff should give careful consideration when posting personal information as to how this might be viewed by pupils and parents, even when the postings are within a 'private' online space.

Access to social networking sites

- Social networking sites should never be accessed during timetabled lessons and other contact with pupils and not normally during school working hours.
- Staff may not use school equipment to access social networking sites.
- If the school chooses to make 'official' use of social networking sites this should only be by authorised individuals.

Posting of images and/or video clips

- Photographic images and/or movie clips of children at the school or past pupils, up to the age of 18, should never be posted unless specific consent has been obtained.
- Photographic images and/or movie clips of school staff should not be posted unless specific consent has been obtained.

Privacy

- Staff should recognise that their existing lists of friends/contacts/followers may include people who are part of both their private and professional lives.
- Staff should never be online 'friends' with children at the school or past pupils up to the age of 18.
- Staff should not create new links with parents at the school, unless there is a professional reason for doing so. In such instances there should be a clear understanding of the purpose of the link and what 'information' the parent will have access to.
- Profile settings should be regularly checked, and updated as necessary, to ensure that posted comments and images are not publicly accessible.
- Any changes to social networking sites and privacy settings should be clearly understood.

Additional considerations

Thought should be given to what the implications of this policy will be for the different groupings within the staff employed at the school, e.g.

- Teacher
- Teaching assistant
- Other support staff, e.g. bursar, site manager, lunchtime supervisors, office staff, cleaners
- Outside agency staff, e.g. sports coaches, music tutors, etc.
- Volunteers, visitors, etc

Appendix 3 – Acceptable Use Agreements

The AUAs included are:

- Pupil Acceptable Use Agreement
- Parent/Carer support for Student/Pupil Acceptable Use Agreement
- Laptop Acceptable Use Agreement
- Staff Acceptable Use Agreement

Pupil Acceptable Use Agreement

For my own personal safety:

- I understand that the school will monitor my use of the IT systems, e-mail and other digital communications.
- I will not tell anyone my username or password nor will I try to use any other person's username and password.
- I will be aware of 'stranger danger', when I am communicating online.
- I will not give out any personal information (e.g. home address and telephone number) about myself or anyone else when online.
- I will not arrange to meet people offline that I have communicated with online.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

Respecting everyone's rights to use technology as a resource:

- I understand that the school IT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school IT systems for online gaming, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

Acting as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- 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 take or distribute images of anyone without their permission.

Keeping secure and safe when using technology in school:

- I will only use approved e-mail or message accounts on the school system.
- I will only use my personal handheld/external devices (e.g. mobile phones, USB devices, etc.) in school if I have permission and I understand that if I do use my own devices in school I must follow the rules as if I was using school equipment.
- I will not try to 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 immediately report any damage or faults involving equipment or software.
- I will not open any attachments to e-mails, unless given permission to do so and I know and trust the person/organisation that sent the e-mail.
- I will ask for permission before sending an e-mail to an external person/organisation
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will immediately tell a staff member if I receive an offensive e-mail or message.

Using the internet for research or recreation:

- When I am using the internet to find information, I should take care to check that the information that I access is accurate.

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).

Taking responsibility for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (e.g. cyberbullying, inappropriate use of images and/or personal information).
- I understand that if I break these rules I will be subject to disciplinary action as outlined in the school's Behaviour Policy. This may also include loss of access to the school network/internet.

I have read and understood the above and agree to follow the rules outlined.

Name:	
Signature:	
Date:	

Parent/Carer support for Pupil Acceptable Use Agreement

The school expects *pupils* to be responsible and safe users of IT. A copy of the *Pupil* Acceptable Use Agreement is attached, so that parents/carers will be aware of the school expectations of young people.

Parents/carers are requested to sign below to show their support of the school in this important aspect of the school's work.

Parent/Carer's Name:	
Pupil's Name:	

As the parent/carer of the above *pupil*, I understand that my son/daughter will have access to the internet and to IT systems at school.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of IT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems. I also understand that although internet filtering systems usually work very well, inappropriate content may occasionally still be accessible, but in this instance the school will take appropriate action with the service provider to request such content is removed.

I understand that my son's/daughter's activity on the IT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signature:	
Date:	

Laptop/Devices Acceptable Use Agreement

1. Introduction

- This agreement applies to all laptops and other associated devices which are loaned to staff and therefore remain the property of the school.
- It should be read in conjunction with the school's Online Safety Policy
- All recipients and users of these devices should read and sign the agreement.

2. Security of equipment and data

- The laptop and any other equipment provided should be stored and transported securely. Special care must be taken to protect the laptop and any removable media devices from loss, theft or damage. Users must be able to demonstrate that they took reasonable care to avoid damage or loss.
- Staff should understand the limitations of the school's insurance cover.
- Government and school policies regarding appropriate use, data protection, information security, computer misuse and health and safety must be adhered to. It is the user's responsibility to ensure that access to all sensitive information is controlled.

3. Software

- Any additional software loaded onto the laptop/device should be in connection with the work of the school. No personal software should be loaded.
- Only software for which the school has an appropriate licence may be loaded onto the laptop/device. Illegal copying of software is subject to civil damages and criminal penalties.
- Users should not attempt to make changes to the software and settings that might adversely affect its use.

4. Faults

- In the event of a problem with the laptop/device, the school's IT Support provider should be contacted.

Declaration:

I have read and understood the above and also the school's Online Safety Policy and agree to abide by the rules and requirements outlined.

Name:	
Signature:	
Date:	

Staff Acceptable Use Agreement

- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I appreciate that IT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail, social networking and that IT use may also include personal IT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Head Teacher.
- I understand that my use of school information systems, internet and e-mail may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware unless authorised, e.g. on a school laptop/device.
- I will ensure that personal data, particularly that of pupils, is stored securely through encryption and password and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the school Online Safety policy.
- I will respect copyright and intellectual property rights.
- I will ensure that electronic communications with pupils (including e-mail, instant messaging and social networking) and any comments on the web (including websites, blogs and social networking) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure that pupil use of the internet is consistent with the school's Online Safety Policy.
- When working with pupils, I will closely monitor and scrutinise what pupils are accessing on the internet including checking the history of pages when necessary.
- I will ensure that computer monitor screens are readily visible, to enable monitoring of what the children are accessing.
- I know what to do if offensive or inappropriate materials are found on screen or printer.
- I will report any incidents of concern regarding pupils' safety to the appropriate person, e.g. Online Safety Co-ordinator, Designated Safeguarding Lead and/or SLT member.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds.

Name:	
Signature:	
Date:	