Acceptable Use of Technology Policy

Early Years and Key Stage 1

- I understand that our school rules will help keep me safe and happy when I go online.
- I only go online when an adult is with me.
- I check with an adult before I click on links or things online.
- I keep my personal information and passwords safe.
- I only send polite and friendly messages online.
- I know the school can see what I am doing online when I use school computers and iPads.
- If I see something online that makes me feel upset, unhappy, or worried, I will always tell an adult as soon as I can.
- I can visit www.ceopeducation.co.uk to learn more about keeping safe online.
- I know that if I do not follow the school rules and values, then access to devices and platforms may be removed. The Positive Relationships Policy and Support Ladder will be followed to support next steps.
- I have read and talked about these rules with my parents/carers.

Acceptable Use of Technology Policy

Key Stage 2

I understand that the school Acceptable Use Policy will help keep me safe and happy online at home and at school.

Safe

- I will be kind and respectful online, just like I am in school.
- I will only share pictures or videos online if they are safe, kind, and I have asked for permission first.
- I will only click on links if I know what they do, or I will ask a safe adult first.
- I will only chat with people I know online, or I will ask a safe adult to help me decide if someone I don't know is safe to speak with online.
- If someone online asks to meet me, I will tell a safe adult straight away.

Learning

- I always ask permission from a safe adult before using the internet.
- I only use websites, tools and/or search engines that my teacher has chosen or given me permission to use.
- I use school devices for school work unless I have been told otherwise.
- If I need to learn online at home, I will follow the same rules in this policy.

True

- I know that some things or people online might not be honest or truthful.
- If I am unsure if something online is true, I will check other websites, books, or ask a safe adult.
- I always credit the person or source that created any work, images, or text I use.
- I will only use Artificial Intelligence (AI) tools when a safe adult says it is allowed.
- I will not put personal information about me or anyone else into AI tools.
- I will not use AI to make fake images, voices, videos or messages about other people.

Responsible

- I keep my personal information safe and private online.
- I will keep my passwords safe and will not share them.
- I will not access or change other people's files or information.
- I will only change the settings on a device if a member of staff has allowed me to.

Tell

- If I see anything online that makes me feel worried, upset, or frightened, I will
- If I am aware of anyone being unkind or unsafe with technology, I will minimise the screen, shut the laptop lid, and tell a safe adult immediately.
- If an AI tool shows me something worrying, unkind, rude, violent, confusing or unsafe, I will stop and tell a safe adult.

- I understand that the adults at school are responsible for keeping me safe; they may need to speak to other safe adults, or my parents/carers, if I tell them about something that has happened online.
- I can visit www.ceopeducation.co.uk and www.childline.org.uk to learn more about being safe online or to seek help

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all school owned devices and networks are checked/monitored to help keep me safe, even if I use them at home. This means someone at the school may be able to see and/or check my online activity when I use school devices and networks if they are worried about my or anyone else's safety or behaviour.
- I understand that my behaviour online can affect others and I will not behave in a way that will upset, frighten or embarrass others.
- I will not bring a mobile phone or other smart device into school with me.
- I have read and talked about these rules with my parents/carers.
- I know that if I do not follow the school rules and values, then access to devices and platforms may be removed. The Positive Relationships Policy and Support Ladder will be followed to support next steps.

Artificial intelligence

- AI means technology that can make or suggest things, like words, pictures, videos, voices, answers or ideas. I will only use AI when an adult says I can.
- I ask an adult before I use AI and ask for their help to use it correctly.
- I will only use AI tools that the school has said I can use and in the wy they have shown me.
- I will not put names, photos, personal information or private information about me or other people into AI tools.
- I understand that AI can help me learn, but it should not do all my work for me.
- I will ask for help if I am not sure whether I can use AI for my work.
- I will not use AI to pretend to be someone else.
- I will not use AI to make fake pictures, voices, videos or messages about people.
- I will not use AI to make anything unkind or upsetting about another person.
- I know that AI can make mistakes, so I will check information with an adult.
- If AI shows me something worrying, unsafe, unkind or confusing, I will stop and tell an adult.

Acceptable Use of Technology Policy

Children with Additional Needs

Safe

- I ask an adult if I want to use the internet.
- I only use phones, tablets or computers when an adult says it is okay.
- I keep my information private on the internet.
- I ask an adult before I take or share a photo, video or message.
- I know that if I do not follow the school rules and values, then I will not be able to use devices, and my parents will have to come to school for a meeting.

Meeting

- I tell an adult if I want to talk to people on the internet.
- If I meet someone online, I talk to an adult.

Accepting

- I do not open messages from strangers.
- I check web links to make sure they are safe.

Reliable

- I make good choices on the internet.
- I check the information I see online.

Tell

- I use kind words on the internet.
- If someone is mean online, then I will not reply. I will save the message and show an adult.
- If I see anything online that worries or upsets me, I will tell a safe adult.

Agreed device use for individual specific needs

- If I use a phone or device to help with my health, communication or support needs, I will use it in the way staff have explained.
- I will only use my device for the specific reason it has been provided or allowed.
- I will not use my device to take photos, record, send messages or go online unless staff have said this is part of my support plan.
- If I need help using my device safely, I will ask a safe adult.
- I understand that having permission to use a device does not mean I can use it for anything I want during the school day.

Remote Learning

- These expectations are in place to help keep me safe when I am learning at home using Microsoft 365 and when meeting via TEAMS.
- I should read and talk about these rules with my parents/carers.
- Remote/online learning will only take place using agreed platforms and during usual school times.
- My use of Microsoft 365 is monitored to help keep me safe.
- Only members of the school community can access Microsoft 365
- I will only use my school provided account login to access remote learning.
- I will use privacy settings as set up the school.
- I will not share my login/password with others.
- I will not share any access links to remote learning sessions with others.
- When taking part in remote/online learning I will behave as I would in the classroom.
- If I am concerned about anything that takes place during remote/online learning, I will speak to a safe adult at home.
- I understand that inappropriate online behaviour or concerns about my or others safety during remote/online learning will be taken seriously just like they would in school.
- When taking part in live sessions I will:
    - mute my video and microphone.
    - wear appropriate clothing and be in a suitable location.
    - ensure backgrounds of videos are neutral and personal information/content is not visible.
    - use appropriate alternative backgrounds.
    - attend the session in full. If for any reason I cannot attend a session in full, I will let my teacher know.
    - I will take part from a suitable location, following any arrangements agreed with the school. I will take reasonable steps to protect my privacy and the privacy of other people in my home.

Acceptable Use of Technology

Parent Agreement

1. I have received and read the Shipbourne School Acceptable Use of Technology Policy (AUP) and have discussed its expectations with my child in a way that is appropriate to their age, understanding and needs.

2. I understand that the AUP explains how my child is expected to use technology safely, kindly, lawfully and responsibly, including when using:
    - [school/setting]-provided devices, accounts, systems and internet access;
    - [school/setting]-provided technology away from the setting;
    - personal devices or services where their use affects the safety or wellbeing of a child or another person, disrupts the safe or effective operation of the [school/setting], or raises a safeguarding or behaviour concern.

3. I understand that access to online content through school devices and systems is appropriately filtered and that use of school provided devices, accounts and systems may be monitored, including when they are used away from the setting. The school has provided information about its filtering and monitoring arrangements in their Child Protection Policy, which I have also read.

4. I understand that filtering and monitoring arrangements help to keep children safe, protect systems and support compliance with relevant policies, but cannot remove every online risk. Monitoring will be proportionate and undertaken in accordance with data protection, privacy and human rights requirements.

5. I am aware that my child must not bring mobile phones and smart devices into school. If my child needs an exception or reasonable adjustment because of a disability, medical condition, communication need or other individual circumstance, I will discuss this with the school so that appropriate arrangements can be considered, agreed and recorded. I will never contact my child directly via a device during the school day.

6. I will support my child to understand and follow the school's expectations for technology use, including social media, mobile phones, online communication, images and recordings and, where relevant, artificial intelligence tools.

7. I will model safe, positive and respectful online behaviour and support my child not to create, post or share content that identifies, targets, threatens, bullies, harasses or risks causing harm to a child, family, member of staff or another member of the school community.

8. If I have a concern or complaint, I am encouraged to use the school's established communication, safeguarding or complaints routes, as appropriate, so that it can be properly considered.

9. I will report concerns about my child's online safety, or online concerns that may affect the safety or wellbeing of another member of the school community, to an appropriate member of staff. This may include my child's class teacher, a Designated Safeguarding Lead or the Headteacher. Where necessary, I may also report the concern to another relevant organisation.

10. If the school has concerns about my child's online safety or behaviour, I understand that these will be considered fairly and proportionately in line with relevant safeguarding, behaviour and other procedures. The school will communicate with me where it is appropriate and safe to do so.

11. I understand my role in helping my child to use technology safely. As appropriate to my child's age, understanding and needs, I will consider the use of parental controls, provide suitable supervision and support, and encourage safe and responsible use of the internet and other technology at home.

12. I know that I can seek online safety information or support from the School by making direct contact or via advice and links on the school website.

Acceptable Use of Technology Policy

Staff, Visitors and Volunteers

As a professional organisation with responsibility for safeguarding, all staff are expected to use technology in a professional, lawful, ethical and responsible manner.

This Staff Acceptable Use of Technology Policy (AUP) sets out the expectations for safe technology use, professional conduct, safeguarding, data protection and system security. It is not intended to unduly limit appropriate teaching, learning or professional use of technology, but to help protect pupils, staff, systems and the wider school community from accidental or deliberate misuse.

All staff are asked to read, understand and agree to adhere to this AUP.

Policy scope

1. I understand that this policy applies to my use of technology systems and services provided by the school or accessed by me as part of my role, both on and offsite. It also applies to personal use of technology where this is linked to my role, involves the school community, uses school systems or information, could affect safeguarding, professional boundaries, confidentiality or data protection, or could reasonably impact on my professional role or the reputation of the school.

2. I understand that the Acceptable Use of Technology Policy (AUP) should be read and followed in line with the child protection policy and staff code of conduct.

3. I am aware that all staff should ensure that technology use is consistent with the school ethos, school staff code of conduct and safeguarding policies, national and local education and child protection guidance, and the law.

Use of school devices and systems

4. I will use school-provided or approved equipment, systems and internet services when working with pupils unless otherwise formally agreed by leaders.

5. I understand that school equipment, systems and internet services are provided for education and professional use. Reasonable personal use is permitted but must not interfere with my work duties, system security, safeguarding, confidentiality or professional boundaries. This permission is at the school's discretion and may be withdrawn at any time.

Data and system security

6. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
    - I will follow the school's requirements for secure passwords, authentication and account access. I will keep authentication information secure and will not share passwords, verification codes or access credentials with others.

- I will protect the devices in my care from unapproved access or theft.

7. I will take care before opening links or attachments, including those apparently sent by a known contact. I will check unexpected or suspicious messages through an appropriate route and report suspected phishing or malicious content to the Headteacher or SNS helpdesk.

8. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the Headteacher or SNS IT support team.

9. I will ensure that any personal data is kept in accordance with data protection legislation, in line with the school information security policies.
    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school.
    - I will only process or share personal data through school-approved systems and services and in line with the setting's data protection and information-security procedures. Any proposed new or changed use of cloud services, AI tools or other online systems involving personal data will be risk assessed and approved through the setting's agreed process before use. Where required, a Data Protection Impact Assessment will be completed.

10. I will not keep documents which contain School related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school learning platform to upload any work documents and files in a password protected environment.

11. I will not store any personal information on the school IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.

12. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

13. I will not attempt to bypass any filtering and/or security systems put in place by the school.

14. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the Headteacher or SNS help desk as soon as possible.

15. If I have lost any school related documents or files, I will report this to the Headteacher as soon as possible.

16. I will follow the School image use policy when taking, using, storing or sharing images or recordings of pupils. Images and recordings must always be appropriate and must only be taken using school-provided or approved equipment. I will not use personal devices, including personal mobile phones, cameras, tablets, smart watches or other wearable technology, to take images or recordings of pupils. Images and recordings will only be taken, used or shared in line with the school image use policy, safeguarding expectations, data protection requirements and consent/lawful basis arrangements.

Classroom practice

17. I understand my role and responsibilities in relation to filtering and monitoring, as explained through induction, safeguarding training and relevant school policies.

18. If I become aware of a filtering or monitoring failure, or witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and/or Headteacher, in line with the school child protection policy.

19. I will follow school expectations for safe technology use in classrooms, remote/online learning and other working spaces, including the use of approved platforms, search tools and AI tools.

20. I will follow the setting's agreed approach to screen use. Any use of screens, devices, apps or online content will be planned, purposeful, age appropriate and supervised, and will not replace face-to-face interaction, play, physical activity, rest, care routines or real-world exploration.

21. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material. Additionally, their use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that:
    - AI tools must only be used responsibly, ethically and where the tool, purpose and use have been approved by leaders. Any new, unapproved or changed use of AI tools will be risk assessed and approved before use, in line with child protection, data protection and professional conduct expectations.
    - I understand that AI-generated content must be checked for accuracy, bias, appropriateness, copyright and safeguarding implications before it is used or shared.
    - I will not enter personal, sensitive, confidential, safeguarding, assessment or special category information, or images of pupils, staff or other identifiable individuals, into any AI tool unless the tool has been approved for that purpose, the use has been risk assessed, consent has been obtained where required, and the leadership team has confirmed that the processing is lawful and appropriate.
    - I will not add or use AI note takers, transcription tools, recording bots or automated meeting summary tools in any meeting, lesson, supervision, training or professional discussion unless this has been agreed in advance by leadership. Where approved, I will ensure that participants are made aware and their use is transparent, proportionate and in line with safeguarding, confidentiality, consent, data protection and information governance expectations.

- I will not use AI to make decisions about pupils, families or staff, including decisions relating to safeguarding, behaviour, SEND, assessment, attendance, admissions, recruitment, allegations or pastoral support, without appropriate professional oversight and in line with setting policy.
- Only approved AI platforms may be used with pupils. Pupils must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
- I will report any concern involving AI misuse, including deepfake or manipulated content, impersonation, harmful AI-generated material, AI-facilitated bullying or harassment, or AI-generated nude/semi-nude imagery, in line with the school child protection, behaviour, anti-bullying, staff conduct and data protection procedures.

22. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
    - creating a safe environment where pupils feel comfortable to report concerns and say what they feel, without fear of getting into trouble or being judged for talking about something which happened to them online.
    - involving the DSL or a deputy as part of planning online safety lessons or activities to ensure support is in place for any pupils who may be impacted by the content.
    - informing the DSL and/or leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
    - making informed decisions to ensure any online safety resources used with pupils are appropriate.

23. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

Mobile phones and smart devices

24. I will ensure that my use of mobile phones and smart devices is compatible with my professional role, does not interfere with my duties, and takes place in line with the staff code of conduct, mobile phone policy and the law.

25. I will model safe and professional use of mobile phones and smart devices and will support the school's expectations for pupils.

26. Where mobile phones or smart devices are used for professional purposes, such as authentication, learning activities, recording rewards or sanctions, or other agreed tasks, I will use school-provided devices where available. Where staff are permitted to use personal devices for professional purposes, this must be formally agreed by the school and managed in line with school policy.

27. Any use of a personal mobile phone or smart device for professional purposes, or in exceptional circumstances, must be transparent, necessary, proportionate and approved by the

Headteacher or other designated leader. Use must not compromise supervision, safeguarding, confidentiality, professional boundaries, data protection or the learning environment.

Online communication, including use of social media

28. I will ensure that my use of communication technology, including social media, is compatible with my professional role, does not interfere with my work duties, and takes place in line with the child protection policy, staff behaviour policy/code of conduct, social media policy and the law.

29. I will protect myself, my professional reputation and the reputation of the school online. I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.

30. My electronic communications with current and former pupils and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
    - I will ensure that all electronic communications take place in a professional manner via school-provided communication channels and systems, such as a school email address, user account or telephone number.
    - I will not use personal accounts, personal profiles, personal phone numbers, private messaging apps, gaming accounts or other personal communication channels to contact or communicate with pupils or their families, unless this has been formally approved, risk assessed and recorded by leaders.
    - I will not share any personal contact information or details with pupils such as my personal address, email address or phone number.
    - I will not share personal information about my private life with [children/pupils/students] online, through messaging, social media, gaming platforms, apps or other digital communication channels. I will maintain appropriate professional boundaries in all digital communication.
    - I will not add, follow, accept or respond to friend requests, direct messages or other personal online communication from current or former pupils, or their parents/carers, where this is linked to my role, the school or could blur professional boundaries. Any attempted contact will be reported to my line manager and/or the DSL.
    - Any pre-existing links, relationships or situations that affect how I apply the AUP or other relevant policies will be discussed with the DSL and/or Headteacher. This is to help safeguard pupils, staff and the wider school community by ensuring professional boundaries, safeguarding expectations and communication arrangements are clear.
    - Where digital communication with pupils or families is required, I will follow the school's expectations about when communication should take place, including any agreed arrangements for out-of-hours contact, emergency communication or role-specific responsibilities.

Policy concerns

31. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, terrorist material or adult pornography covered by the Obscene Publications Act.

32. I will not access, create, transmit, display, publish, forward, discuss, send, share or show any material or content that may be harmful, inappropriate, adult, offensive, unprofessional, or likely to harass, cause offence, inconvenience or needless anxiety to any other person. This applies when using school systems, school devices, personal devices, personal accounts, messaging apps, online platforms, social media or shared spaces. It includes content shared in staff rooms, offices, online groups or other staff communication spaces, where this takes place on school premises, during working time, or in any context linked to my role.

33. I will not engage in online or digital behaviour linked to my role that compromises safeguarding, professional boundaries, confidentiality, data protection, public confidence in my professional conduct or my ability to carry out my role.

34. I will report and record any concerns about the welfare, safety or behaviour of pupils or parents/carers online to the DSL in line with the school child protection policy.

35. I will report concerns about the welfare, safety, conduct, or behaviour of staff, including online, digital, device-related or technology-linked concerns, to the Headteacher in line with the school child protection policy, staff behaviour policy/code of conduct, low-level concerns procedures and/or allegations against staff policy.

Policy compliance and breaches

36. If I have any queries or questions regarding safe and professional practice online, either in school or off site, I will raise them with the DSL and/or the Headteacher.

37. I understand that the school may exercise its right to monitor the use of its devices and information systems to check policy compliance and help ensure the safety of pupils and staff.
    - This includes monitoring all school-provided devices and school systems and networks including school-provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school-provided devices, systems and/or networks.
    - This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

    - Staff will be informed about the nature, purpose and extent of monitoring through this AUP, relevant policies, privacy information and/or staff guidance.

38. I understand that if the school believes that unauthorised and/or inappropriate use of school devices, systems or networks is taking place, the school may invoke its disciplinary procedures as outlined in the staff behaviour code of conduct.

39. If I find myself in a situation where my online contact, device use, recording, image use or AI use could be misinterpreted, I will report this promptly to the DSL and/or Headteacher so it can be recorded and managed transparently.

40. Any breach or concern involving online contact, device use, images, recordings, social media, AI use, confidentiality, data protection or professional boundaries must be reported to the Headteacher and/or DSL without delay, even if it appears minor, accidental or unlikely to meet the harm threshold.

41. I understand that if the school believes that unprofessional or inappropriate online or technology-related activity may have compromised safeguarding, professional boundaries, confidentiality, data protection, public confidence in professional conduct or my ability to carry out my role, the concern will be considered fairly, proportionately and confidentially, in line with relevant safeguarding, staff behaviour, low-level concerns, allegations, data protection and disciplinary procedures. Where the concern may meet the harm threshold, advice will be sought and/or a referral made to the Local Authority Designated Officer (LADO) in line with local allegations procedures. Where it does not meet this threshold, it will still be recorded and responded to appropriately.

42. Where a concern involves personal data, confidential information, safeguarding information, images, recordings, AI tools, transcription tools or unauthorised sharing, the DPO/data protection lead will be informed promptly so that any data protection, information governance or reporting requirements can be considered.

43. I understand that if the school suspects criminal offences have occurred, the police will be informed where appropriate.

44. I understand that this AUP cannot cover every possible situation. If I am unsure whether any use of technology, online communication, image use, recording, personal device use, social media, AI tool or digital contact is appropriate, I will seek advice from the DSL and/or Headteacher before taking action. I will act in a way that safeguards pupils, protects professional boundaries, and is open to scrutiny.

Remote Learning

Leadership oversight and approval

1. Remote/online learning will only take place using Microsoft 365 which has been assessed and approved by Headteacher and Governing Board.

2. Staff will only use school approved professional accounts with pupils and/or parents/carers.
    - Use of any personal accounts to communicate with pupils and/or parents/carers is not permitted.
        - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the Headteacher.
    - Staff will use work provided equipment where possible. If personal devices are to be used, this must be agreed with the Headteacher in advance and only school issued Microsoft accounts must be used.

3. Online contact with pupils and/or parents/carers will not take place outside of school learning hours.

4. All remote/online lessons will be formally timetabled and may be observed by a member of the school SLT.

Data Protection and Security

5. Any personal data used by staff and captured by Microsoft 365 when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.

6. All remote/online learning and any other online communication will take place in line with current school confidentiality expectations.
7. Participants will be informed about any activity that records or retains information such as attendance, chat messages, shared files, audio or video recordings, and how this information will be used.
8. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements.
9. Only members of the school community will be given access to Microsoft 365.

10. Access to Microsoft 365 will be managed in line with current IT security expectations.

11. AI note takers, transcription tools, recording bots or automated meeting summaries must not be used in remote/online learning, meetings or training unless this has been approved in advance by leaders and is managed in line with safeguarding, consent, confidentiality and data protection requirements.

Session management

12. Staff will record the length, time, date, and attendance of any sessions held.

13. Appropriate privacy and safety settings will be used to manage access and interactions.

14. Live sessions will follow the school's agreed staffing, oversight and audit arrangements.

15. Live 1:1 sessions will only take place with approval from the Headteacher and parent/carer.

16. A pre-agreed email detailing the session expectations will be sent to those invited to attend.
    - Access links should not be made public or shared by participants.
    - Pupils and/or parents/carers should not forward or share access links.
    - Staff will explain any expectations about the location from which pupils take part. These will reflect their age, needs, privacy, home circumstances and the nature of the session.

17. Alternative approaches and/or access will be provided to those who do not have access.

Behaviour expectations

18. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.

19. All participants are expected to behave in line with existing school policies and expectations.
    - Appropriate language will be used by all attendees.
    - Staff will not take or record images for their own personal use.
    - Setting decisions about if other attendees can or cannot record events for their own use, and if so, any expectations or restrictions about onward sharing.

20. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.

21. When sharing videos and/or live streaming, participants are required to:
    - wear appropriate dress.
    - ensure backgrounds of videos are neutral (blurred if possible).
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.

22. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

23. Participants are encouraged to report concerns during remote and/or live-streamed sessions:

24. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to the Headteacher.

25. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.

26. Sanctions for deliberate misuse may include restricting/removing use and seeking police or other appropriate advice where behaviour may be unlawful or presents a risk to safety.

27. Any safeguarding concerns will be reported to the Designated Safeguarding Lead, in line with our child protection policy.

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for safeguarding children, all users must understand the boundaries and expectations when using the school Wi-Fi. Users are expected to use Wi-Fi safely, lawfully and responsibly, and to take reasonable steps to protect devices, data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list. All users are reminded that technology use should be consistent with the school ethos, relevant policies and the law.

1. The school provides Wi-Fi to all staff, pupils and approved visitors

2. Use of the Wi-Fi falls under the Acceptable Use of Technology Policy (AUP), the child protection policy, behaviour policy/code of conduct, data protection/security policies and any other relevant policies. All pupils/students, staff, visitors and volunteers using the Wi-Fi must comply with these expectations.

3. The school reserves the right to limit, restrict, withdraw or manage Wi-Fi access where necessary to maintain safeguarding, security, network reliability or fair use of network resources.

4. School owned information systems, including Wi-Fi, must be used lawfully. I understand that the Computer Misuse Act 1990 makes it a criminal offence to gain unauthorised access to computer material, gain unauthorised access with intent to commit or facilitate further offences, or modify computer material without authorisation.

5. I will take reasonable steps to ensure that any personal device connected to school Wi-Fi is appropriately secure, for example by using security updates, antivirus protection where appropriate, and secure passwords/PINs.

6. I will respect system security and will not share passwords, Wi-Fi access details or security information. I will not attempt to bypass school security, filtering or monitoring systems, or download unauthorised software, applications or files.

7. I will not use school Wi-Fi to access, create or share illegal or harmful content, compromise another person’s safety or privacy, interfere with systems, or breach relevant school policies.

8. I will not use school Wi-Fi to access, store, send or share confidential, personal or safeguarding information unless this has been specifically authorised and is in line with school data protection and safeguarding procedures.

9. Staff using school Wi-Fi on personal devices remain subject to the staff behaviour policy/code of conduct, Staff AUP, mobile phone/smart device policy, data protection expectations, and relevant safeguarding and disciplinary procedures.

10. The school takes reasonable and proportionate steps to manage the security of its Wi-Fi service. However, no wireless or internet service can be guaranteed to be free from all risk. Where personal devices are permitted to connect to the school Wi-Fi, users do so at their own

discretion and are expected to keep their devices secure. Any concerns about Wi-Fi security, filtering, monitoring or device safety should be reported to the DSL or identified technical contact.

11. I will report any online safety concerns, filtering breaches, security concerns, or access to inappropriate materials to the DSL and/or Headteacher as soon as possible. I

12. I understand that activity carried out through school Wi-Fi may be monitored and recorded to check policy compliance, protect systems and help keep users safe, including where the Wi-Fi is accessed using a personal device. This does not mean that the school can monitor other activity or information held on the personal device. Monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

13. If the school suspects that unauthorised or inappropriate use, unacceptable behaviour, a data protection concern, a safeguarding concern or criminal activity may have taken place, access may be restricted or withdrawn and the concern may be managed in line with relevant School procedures. Where appropriate, this may include informing the DSL, Data Protection Officer, Headteacher, LADO or police.