HILDENBOROUGH CHURCH OF ENGLAND PRIMARY SCHOOL

"I can do all things through Christ who strengthens me," (Philippians 4:13) so that I can be the best that I can be, for myself, for others and for God.

ACCEPTABLE USE OF TECHNOLOGY POLICY

September 2025

We aspire for our community to flourish as we journey together to fulfil our God given potential by encouraging a delight in the pursuit of wisdom and knowledge. We cherish each person as unique and special, and celebrate God's creation through providing rich experiences, which enlighten, challenge, shape and enhance life's opportunities for all.

Last Reviewed	September 2024
Next Review Date	September 2026
Ratified by	FGB
Ratified on	24.09.2025
Lead Person	Ruth Ardrey

Purpose

As a professional organisation with responsibility for safeguarding, all members of staff, visitors, volunteers, children and parents/carers are expected to use Hildenborough Primary IT systems in a professional, lawful, and ethical manner. To ensure that members of all stakeholders understand their professional responsibilities and/or ways to keep safe, when using technology and access appropriate resources, we ask that all stakeholders read and understand the content of this policy.

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they or any other stakeholder use the internet personally. However, the AUP will help ensure that all staff understand Hildenborough's expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

AUP Statements for Early Years and Key Stage 1 (0-6)

- I understand that the school Acceptable Use Policy will help keep me safe and happy online.
- I only use the internet when an adult is with me.
- I only click on online links and buttons when I know what they do. If I am not sure, I ask an adult first.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online when I use school computers/tablets and systems learners are expected to use, including if I use them at home.
- I always tell an adult if something online makes me feel upset, unhappy, or worried.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
- I know that if I do not follow the school rules:
    - I might be banned from using them in the future
    - I might need to be accompanied by an adult 1:1 in the future
- I have read and talked about these rules with my parents/carers.

AUP Statements for Key Stage 2 (7-11)

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

Safe

- I only send messages which are polite and friendly
- I will only post pictures or videos on the internet if they are appropriate, and if I have permission

"I can do all things through Christ who strengthens me," (Philippians 4:13) so that I can be the best that I can be, for myself, for others and for God.

- I only talk with and open messages from people I know, and I only click on links if I know they are safe
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult

Trust

- I know that not everything or everyone online is honest or truthful
- I will check content on other sources like other websites, books or with a trusted adult
- I always credit the person or source that created any work, image or text I use
- I will not use Artificial Intelligence (AI) to create words, pictures or other resources and submit the work as my own.

Responsible

- I always ask permission from an adult before using the internet
- I only use websites and search engines that my teacher has chosen
- I use school computers for school work, unless I have permission otherwise
- Smart mobile phones are not permitted at all. Non- smart phones are not permitted unless I walk to school in Year 6. If this is the case, then I know I need to give this into my teacher to be looked after for the day.
- I will only access age-appropriate apps on my mobile phone device and these will not be accessed at school
- I keep my personal information safe and private online
- I will keep my passwords safe and not share them with anyone
- I will not access or change other people's files or information
- I will never change the settings on a computer.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of school devices/computers and internet access will be monitored
- If, for curriculum reasons, I need to bring a personal device, for example a laptop into school, then I will use it in line with my school's device.
- If I am in Year 5 or 6 and I bring my non- smart mobile phone to school, I understand that it must remain on silent in the school office for the duration of the day.
- I have read and talked about these rules with my parents/carers
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online
- I know that if I do not follow the school rules then my teacher or the Headteacher will speak to my parents.
- I understand that the school can issue me with a consequence if I do certain unacceptable things online, even if I'm not in school when I do them

Tell

- If I am aware of anyone being unsafe with technology, I will report it to a teacher
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page and tell an adult straight away, and turn off the screen.

AUP Statements for Learners with Special Educational Needs and Disabilities (SEND)

Learners with SEND functioning at Levels P4 –P7

- I ask a grown-up if I want to use the computer.
- I make good choices on the computer.
- I use kind words on the internet.
- If I see anything that I do not like online, I tell a grown up.
- I know that if I do not follow the school rules then:
    - I might be banned from using them in the future
    - I might need to be accompanied by an adult 1:1 in the future

AUP Statements for Learners with Special Educational Needs and Disabilities (SEND) Learners functioning at Levels P7+ (Based on Childnet's SMART Rules)

Safe

- I ask a grown up if I want to use the computer.
- I do not tell strangers my name on the internet.
- I know that if I do not follow the school rules then:
    - I might be banned from using them in the future
    - I might need to be accompanied by an adult 1:1 in the future

Meeting

- I tell a grown-up if I want to talk on the internet.

Accepting

- I do not open messages or emails from strangers.

Reliable

- I make good choices on the computer.

Tell

- I use kind words on the internet.
- If I see anything that I do not like online, I will tell a grown up.

"I can do all things through Christ who strengthens me," (Philippians 4:13) so that I can be the best that I can be, for myself, for others and for God.

AUP Acknowledgement Statements for Parents/Carers

Agreement

1. I have read and discussed Hildenborough CE Primary School pupil acceptable use of technology policy (AUP) with my child and understand that the AUP will help keep my child safe online.

2. I understand that the AUP applies to my child's use of school devices and systems on site and at home including (iPads, laptops, IT suite computers), and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another pupil, could have repercussions for the orderly running of the school, if a child is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.

3. I understand that any use of school devices and systems are appropriately filtered; this means that all key words, history or searches are monitored via a Netsweeper report which is periodically sent to DSL/ Headteacher to review and monitor individuals use.

4. I am aware that my child's use of school provided devices and systems will be monitored for safety and security reasons, when used on and offsite. This includes checking the history of each device spontaneously. Monitoring approaches are in place to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

5. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use school devices and systems, on and offsite. I however, understand that the school cannot ultimately be held responsible for filtering breaches that occur due to the dynamic nature of materials accessed online, or if my child is using a personal device, including mobile or smart technologies.

6. I am aware that the school mobile and smart technology policy states that my child cannot use personal devices, including mobile and smart technology on site. Instead, they must be given to my class teacher and will be stored securely in the main office.

7. I understand that if my child has a mobile phone device, that I will not allow them to download apps that are not suitable for their age and I will check the usage of said mobile phone to ensure my child is using it safely.

8. I am aware that the school allows the use of cameras for personal use eg- plays, sports events, assemblies, etc. I know for the safety of all children, I must not upload any images to social media to protect all children.

9. I understand that my child needs a safe and appropriate place to access remote/online learning, for example, if the school is closed. I will ensure my child's access to remote/online learning is appropriately supervised and any use is in accordance with the school remote learning AUP.

10. I and my child are aware of the importance of safe online behaviour and will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the school community, or content that could adversely affect the reputation of the school.

11. I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety online.

12. I will inform the school (for example speaking to a member of staff and/or the Designated Safeguarding Lead) or other relevant organisations if I have concerns over my child's or other members of the school community's safety online.

13. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.

14. I understand my role and responsibility in supporting the school online safety approaches and safeguarding my child online. I will use parental controls, supervise access and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Acceptable Use of Technology for Staff, Visitors and Volunteers Statements

Staff Acceptable Use of Technology Policy (AUP)

Policy scope

- I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school or accessed by me as part of my role within Hildenborough CE Primary School, professionally and personally, both on and offsite. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email, data and data storage, remote learning systems and communication technologies.

- I understand that Hildenborough CE Primary School's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school child protection/online safety policy and staff code of conduct.

- I am aware that this AUP does not provide an exhaustive list; 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

1. I will only use the equipment and internet services provided to me by the school for example school provided laptops, tablets, mobile phones and internet access, when working with pupils.

2. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed; but can be revoked at any time.

Data and system security

3. 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 use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system. Passwords should be changed at least termly.
    - I will protect the devices in my care from unapproved access or theft. Devices should not be left visible out of school times.

4. I will respect school system security and will not disclose my password or security information to others.

5. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager: Jez Hoare, SNS UK.

6. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager: Jez Hoare, SNS UK

7. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK GDPR 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: password protection.

8. 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 or school approved/provided VPN.

9. 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.

10. 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.

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

12. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Support Provider: Jez Hoare, SNS UK as soon as possible.

13. If I have lost any school related documents or files, I will report this to the ICT Support Provider/Team/lead (Jez Hoare) and school Data Protection Officer (Ruth Ardrey) as soon as possible.

14. Any images or videos of children will only be used as stated in the school camera and image use policy. I understand images of children must always be appropriate and should only be taken with school provided equipment and only be taken/published where children or parent/carers have given explicit written consent.

Classroom practice

15. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by Hildenborough CE Primary School as detailed in the child protection policy and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.

16. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT provider: Jez Hoare, in line with the school child protection policy.

17. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in child protection policy, AUP, mobile phone and social media policy.

18. 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 and/or be judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) (Ruth Ardrey) or a deputy (Emma Welch, Rachel Forward and Caroline Stone) 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.
    - make informed decisions to ensure any online safety resources used with pupils is appropriate.

19. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

Mobile devices and smart technology

20. I have read and understood the school mobile and smart technology and social media policies which addresses use by pupils and staff.

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

22. Visitors/ parents: I will ensure that if I do use my own personal device to take photographs during a play/ sports event/ assembly, etc, I will not upload them to my own social media account.

Online communication, including use of social media

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

24. As outlined in the staff code of conduct and school social media policy:
    - I will take appropriate steps to protect myself and my reputation, and the reputation of the school, online when using communication technology, including the use of social media.
    - I will not discuss or share data or information relating to pupils, staff, school, business or parents/carers on social media.

25. My electronic communications with current and past 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 approved and/or provided communication channels and systems, such as a school email address, user account or telephone number. I will not share any personal contact information or details with pupils, such as my personal email address or phone number.
    - I will not add or accept friend requests or communications on personal social media with current or past pupils and/or their parents/carers.
    - If I am approached online by a current or past pupils or parents/carers, I will not respond and will report the communication to my line manager and (Ruth Ardrey) Designated Safeguarding Lead (DSL).
    - Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL and/or headteacher.

Communications: emails specifically

The school has a legal duty to ensure that important information within emails is retained securely for future reference. Staff working in all roles within the school must understand how to 'file' emails and must manage their email accounts carefully, in line with GDPR requirements.

Secure retention of emails

Where emails contain crucial information, they must be appropriately filed within staff or student records, or within the school's database (CPOMS). Staff are expected to make reasonable decisions about what may constitute information within an email which needs to be formally filed for future reference.
Whilst it is not possible to provide a complete list, the following examples will support staff to be able to make a reasonable and informed decision about the content of an email and whether it needs to be filed as part of the school's formal record:

1. any email which includes information considered to be relevant to safeguarding. These emails should be attached to records within the electronic safeguarding system (CPOMS).
2. information regarding a child's education needs including special educational needs
3. information which may influence future decision making by teachers, curriculum leaders or members of the leadership team.
4. information that raises a concern about the school's actions or provision which cannot be resolved by a member of staff informally (at Stage 1 of the complaints procedure). Staff are expected to ensure that information which should be retained within the school's formal records and database is transferred to this secure record in a timely manner, and within one month of it being sent or received.

Deletion of Emails

External emails which are not reasonably considered to require formal filing, and which do not fall within the legal requirements for retention by the school, should be deleted within 30 days. This includes routine communication with parents and other stakeholders about school provision and responses to enquiries which do not constitute formal complaints. Deletion of emails will ensure that data is not kept for longer than is necessary, in line with GDPR requirements. Staff are expected to use their professional judgement

to decide what should be retained and what can reasonably be deleted. Where needed, staff may seek further advice from their line manager or the Headteacher of the school about whether or not an email should be retained. All staff are expected to manage their emails (mailboxes) in line with this policy and to delete emails which are not retained as part of the school's secure records or files after 30 days.

Policy concerns

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

27. I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

28. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

29. 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.

30. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with school child protection policy and the allegations against staff policy.

Policy Compliance and Breaches

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

32. I understand that the school may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to 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.

33. I understand that if the school believe 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 code of conduct.

34. I understand that if the school believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the staff code of conduct.

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

"I can do all things through Christ who strengthens me," (Philippians 4:13) so that I can be the best that I can be, for myself, for others and for God.

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school boundaries and requirements when using the school Wi-Fi systems and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.
This is not an exhaustive list, and all members of the school community are reminded that technology use should be consistent with our ethos, other appropriate policies, and the law.

1. The school provides Wi-Fi for the school community and allows access for visitors for an educational point of view or meetings eg- PTA, Governors, external agencies.

2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the school premises that is not the property of the school.

3. The use of technology falls under Hildenborough CE Primary School Acceptable Use of Technology Policy (AUP), child protection policy and behaviour which all pupils /staff/visitors and volunteers must agree to and comply with.

4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. School owned information systems, including Wi-Fi, must be used lawfully; 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.

6. I will take all practical steps necessary to make sure that any equipment connected to the school service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The school wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

10. I will not attempt to bypass any of the school security and filtering systems or download any unauthorised software or applications.

11. My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Ruth Ardrey) as soon as possible.

14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead/ Headteacher (Ruth Ardrey).

15. I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

"I can do all things through Christ who strengthens me," (Philippians 4:13) so that I can be the best that I can be, for myself, for others and for God.

Acceptable Use Policy (AUP) for Remote/Online Learning

Our Acceptable Use Policy for remote learning is set out below. This is to be used in the instance of children having to complete their learning at home, e.g. during a long term absence or a class closure or whole school closure. These statements also apply to if/when they use Microsoft Teams or Tapestry to complete home learning tasks. Parents are required to read this policy and discuss the rules below with their child (at an age-appropriate level) so that they understand what is expected of them.

Remote/Online Learning AUP– Pupil Statements

1. I understand that:
    - These expectations are in place to help keep me safe when I am learning at home using Tapestry (Year R and Year 1) and Microsoft Teams.
    - Remote learning will only take place using Microsoft Teams and Tapestry and during the usual hours of the school day (8.35am-3.15pm). However, Home Learning tasks can be posted on Tapestry and Microsoft Teams outside of these hours.
    - My use of Microsoft Teams and Tapestry is monitored by my class teacher to help keep me safe.
    - In the instance of teachers using Microsoft Teams to deliver live lessons from their homes, or on their own, lessons will be recorded for safeguarding purposes. These will be stored securely on Streams and will accessed by members of our class and DSLs (Designated Safeguarding Leads) only.

2. Only members of Hildenborough CE Primary School can access Microsoft Teams and Tapestry. When using these systems, we will follow the following rules:
    - I will only use my provided login details to access remote learning.
    - I will not share my login/password with others.

3. When taking part in remote learning on Microsoft Teams, I will behave as I would in the classroom. This includes:
    - listening to my teacher carefully and following their instructions.
    - not talking when others are talking.
    - being kind and respectful to our peers, e.g. we only make kind comments to each other.
    - use appropriate language.

4. When taking part in live sessions on Microsoft Teams, I will:
    - mute my microphone when asked to by my teacher. I will only unmute myself when my teacher asks me to.
    - only mute my own microphone and not anyone else's.
    - be in a communal area (where there are adults present).
    - have a neutral background or use appropriate alternative backgrounds (only if permitted by the class teacher).

5. When accessing home learning tasks, posting on the class posts page or during a class chat, I will:

- use appropriate language.
- post kind comments only
- use appropriate images, GIFs and emojis.
- think before I click (remember anything you post can be seen by others, including our class teachers).
- only edit/delete work or comments I post, e.g. I will not purposefully delete folders or work posted by my teacher or other members of my class.

6. If I am concerned about anything that takes place during remote learning, I will:
    - tell an adult straight away, e.g. my parents or my class teacher.

7. I understand that inappropriate online behaviour or concerns about my safety during remote learning will be taken seriously. This could include:
    - being removed from Microsoft Teams or Tapestry.
    - informing my parents.
    - reflection time.

Remote/Online Learning AUP- Staff Statements

The Remote/Online Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of school community when taking part in remote/online learning, for example following any full or partial school closures.

Leadership oversight and approval

1. Remote/online learning will only take place using Microsoft Teams and Zoom (as back up).
    - Microsoft Teams has been assessed and approved by a member of Senior Leadership Team (SLT).

2. Staff will only use school managed professional accounts with pupils and 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 Ruth Ardrey, Designated Safeguarding Lead (DSL).
    - Staff will use work provided equipment where possible, for example, a school laptop, tablet, or other mobile device. Other devices will need permission from Ruth Ardrey, Headteacher.

3. Online contact with pupils and parents/carers will not take place outside of the operating times as defined by SLT:
    - 8:35am- 3:15pm Monday-Friday

4. All remote/online lessons will be formally timetabled**;** a member of SLT is able to drop in at any time.

5. Live-streamed remote/online learning sessions will only be held with approval and agreement from a member of SLT.

Data Protection and Security

6. All remote/online learning and any other online communication will take place in line with current school confidentiality expectations as outlined in Staff Code of Conduct policy.

7. Staff will not record lessons or meetings, unless previously agreed by SLT.

8. Only members of the school community will be given access to Microsoft Teams.

9. Access to Microsoft Teams will be managed in line with current IT security expectations as outlined in child protection policy and our AUP (this policy).

Session management

10. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
    - limiting chat
    - limiting share screen function to only necessary
    - keeping meeting IDs private,
    - use of waiting rooms or equivalent- for meetings.

11. Live 1:1 sessions will only take place with approval from the headteacher and this should be done with a member of SLT, or a parent/carer is in the room.

12. A pre-agreed invitation detailing the session expectations will be sent to those invited to attend.
    - Access links should not be made public or shared by participants, via class teams.
    - Pupils or parents/carers should not forward or share access links.
    - If pupils or parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
    - Pupils are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.

13. Alternative approaches (where possible) will be provided to those who do not have access.

Behaviour expectations

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

15. All participants are expected to behave in line with existing school policies and expectations. This includes:
    - Appropriate language will be used by all attendees.
    - Staff will not take or record images for their own personal use.
    - Pupils will not take or record images for their own personal use.

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

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

18. 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

19. Participants are encouraged to report concerns during remote sessions:
    - Children should report to their parents/carer or class teacher via Teams communications.

20. 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 Ruth Ardrey, Headteacher or Emma Welch, Deputy Headteacher.

21. 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.

22. Sanctions for deliberate misuse may include restricting/removing use, contacting police if a criminal offence has been committed.

23. Any safeguarding concerns will be reported to Ruth Ardrey, Designated Safeguarding Lead, in line with our child protection policy.