

Barming Pre-School and Primary School

Part of the Orchard Academy Trust



Acceptable Use of Technology Policies

Headteacher: Mr C. Laker

Chair of Governing Body: Rev W North

Date Policy Adopted:	September 2025 Agreed at Governor Level: Tuesday 23 rd September 2025
Policy Review Date:	September 2026
Signature of Chair of Governors:	Rev W. North
Signature of Headteacher:	Mr C. Laker
Policy Author: Senior Leader Responsibility for/ Subject Leader Responsible for:	Name: H Rootes Responsible for: Teaching and Learning

Acceptable Use of Technology Policies (AUPs)

This policy is made of statements that all parties will sign to agree.

Pupil Acceptable Use of Technology Policy

Early Years and Key Stage 1 (0-6)

- I understand that the **Barming Pre-School and Primary School** rules will help keep me safe and happy when I go online
- I only go online when a member of staff is with me.
- I only click on online things online when I know what they do. If I am not sure, I ask a member of staff first.
- 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/tablets, including if I use them at home.
- If I see something online that makes me feel upset, unhappy, or worried I will always tell a member of staff.
- 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 I will not be allowed to use the school technology until I do.
- I have read and talked about these rules with my parents/carers.

Pre-School version

- I only go online with a grown-up.
- I am kind online.
- I keep information about me safe online with adult help.
- I tell a grown-up if something online makes me unhappy or worried.

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 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 a trusted adult says they are safe.
- I know that people online might not be who they say they are. I will only chat with people I know or who a trusted adult says are safe.

- If someone online asks to meet me, I will tell a trusted adult straight away.

Learning

- I will not use any personal devices in school.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen or given me permission to use.
- I use school devices for schoolwork unless I have permission otherwise.
- If I need to learn online at home, I will follow the school remote/online learning AUP.

Trust

- I know that some things or people online might not be honest or truthful.
- If I'm not sure something online is true, I will check with other websites, books, or ask a trusted adult.
- I always credit the person or source that created any work, images, or text I use.
- I will use Artificial Intelligence (AI) tools safely and sensibly. I won't use them to cheat, copy other people's work, or say anything unkind. I know that AI tools can sometimes make mistakes. I will only use them when a teacher or trusted adult says it's okay.

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 I should not or if I see something online that makes me feel worried or upset, I will turn off the screen, close the lid or place the IPAD facedown. I will then get an adult.
- If I am aware of anyone being unsafe with technology, I will report it to an adult at school.
- I know it is not my fault if I see something upsetting or unkind online.
- If I'm not sure about something online or it makes me feel worried or scared, I will talk to a trusted adult.

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/or networks if they are worried about my or anyone else's safety or behaviour.
- If, for any reason, I need to bring a personal device, like a smart/mobile phone and/or other wearable technology into school then I know that it is to be handed in to the class teacher and then collected at the end of the school day. Smartwatches that do not connect to the internet maybe worn only.

- I have read and talked about these rules with my parents/carers.
- I can visit www.ceopeducation.co.uk and www.childline.org.uk to learn more about being safe online or to see help.
- I know that if I do not follow the school rules then there will be appropriate consequences.

Pupils with Special Educational Needs and Disabilities (SEND)

Learners with SEND

- 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.
- I do not open messages or emails from strangers
- I keep my information private 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 appropriate sanctions will take place.

Pupil Acceptable Use Policy Agreement Form

I, with my parents/carers, have read and understood the school Acceptable Use of Technology Policy (AUP).

I agree to follow the AUP when:

1. I use school devices and systems both on site and at home.
2. I use my own equipment out of the school, including communicating with other members of the school or when accessing school systems.

Name..... Signed.....

Class..... Date.....

Parent/Carer's Name.....

Parent/Carer's Signature.....

Date.....

Parent/Carer Acceptable Use of Technology Policy

1. I have read and discussed **Barming Pre-School and 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 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 pupil is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.
3. I am aware that use of mobile and smart technology, such as mobile phones by children, is not permitted at **Barming Pre-School and Primary School**.
4. I understand that any use of school devices and systems are appropriately filtered by a Company called '**ATS**'.
5. 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. 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.
6. 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 understand however, that the school cannot ultimately be held responsible for filtering breaches that occur due to the dynamic nature of materials accessed online.
7. I am aware 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.
8. 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.
9. My child and I 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.

10. 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.

11. 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.

12. 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.

13. I understand that if I or my child do not abide by the Barming Pre-School and Primary School AUP, appropriate action will be taken. This could include sanctions being applied in line with the school policies and if a criminal offence has been committed, the police being contacted.

Child's Name..... Child's Signature
(If appropriate)

Class.....Date.....

Parent/Carer's Name.....

Parent/Carer's Signature.....

Date.....

Acceptable Use of Technology for Staff, Visitors and Volunteers Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use **Barming Pre-School and Primary School** IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for pupils, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand **Barming Pre-School and Primary School** 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.

Policy scope

1. 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 **Barming Pre-School and 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.
2. I understand that **Barming Pre-School and Primary School** Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school Safeguarding and Child Protection policy, Trust Staff Code of Conduct and Remote/ AUP.
3. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the school ethos, Trust 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 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 children.

5. 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; This use is at the school's discretion and can be revoked at any time.
6. Where I deliver or support remote/online learning, I will comply with the schools remote learning AUP.

Data and system security

7. 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 or is a combination of 3 unrelated words and is only used on one system.
 - I will protect the devices in my care from unapproved access or theft. I will not leave any devices visible or unsupervised in public places.
8. I will respect school system security and will not disclose my password or security information to others.
9. 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.
10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.
11. 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, will be suitably protected. This may include data being encrypted by a method approved by the school.
12. 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 SharePoint to upload any work documents and files in a password protected environment.
13. 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.

14. 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.
15. I will not attempt to bypass any filtering and/or security systems put in place by the school.
16. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the **ATS** as soon as possible.
17. If I have lost any school related documents or files, I will report this to **ATS** and school **Data Protection Officer Mr C Howard – Satswana Ltd** as soon as possible.
18. Any images or videos of pupils will only be used as stated in the school camera/IPADs and image use policy. I understand images of pupils must always be appropriate and should only be taken with school provided equipment and only be taken/published where pupils and/or parent/carers have given explicit written consent.

Classroom practice

19. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by **Barming Pre-School and Primary School** as detailed in our Safeguarding and Child Protection policy, and as discussed with me as part of my induction and/or ongoing Safeguarding and Child Protection staff training.
20. 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 (**ATS**), in line with the school Safeguarding and Child Protection policy.
21. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in Safeguarding and Child Protection and Remote learning AUP.
22. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I also 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, its use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that:
 - o AI tools are only to be used responsibly and ethically, and in line with our school child protection, data protection, and professional conduct/behaviour policy expectations.

- o A risk assessment will be undertaken, and written approval will be sought from the senior leadership team prior to any use of AI tools, for example if used in the classroom, or to support lesson planning.
- o A Trust Data Protection Impact Assessment (DPIA) will always be completed prior to any use of AI tools that may be processing any personal, sensitive or confidential data and use will only occur following approval from the DPO.
- o I am required to critically evaluate any AI-generated content for accuracy, bias, and appropriateness before sharing or using it in educational contexts.
- o AI must not be used to replace professional judgement, especially in safeguarding, assessment, or decision-making involving children.
- o Only approved AI platforms may be used with children. Children must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
- o Any misuse of AI will be responded to in line with relevant school policies, including but not limited to, anti-bullying, staff and pupil behaviour and Safeguarding and Child protection.

23. I will promote online safety with the children 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:

- o exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
- o creating a safe environment where children 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.
- o involving the Designated Safeguarding Lead (DSL) (**Miss H Rootes**) or deputies (**Mr C Laker, Mrs A Collie, Miss H Cook, Mrs N Murray, Miss J Russell and Mrs B Deyssel**) as part of planning online safety lessons or activities to ensure support is in place for any children who may be impacted by the content.
- o 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.
- o make informed decisions to ensure any online safety resources used with children are appropriate.

24. 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 Devices and Smart Technology

25. I have read and understood the School Social Media and Smart Technology policies which addresses use by pupils and staff.
26. 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 Trust Staff Code of Conduct and the school Social Media and Smart Technology policy and the law.

Online Communication, including use of Social Media

27. 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 Safeguarding and Child Protection policy, Trust Staff Code of Conduct, Social Media and Smart Technology policy and the law.
28. As outlined in the Trust Staff Code of Conduct and school Social Media and Smart Technology policy:
- a. 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.
 - b. I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.
29. 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.
- a. 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.
 - b. I will not share any personal contact information or details with pupils, such as my personal email address or phone number.
 - c. I will not add or accept friend requests or communications on personal social media with current or past pupils and/or their parents/carers.
 - d. 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 (Miss H Rootes) Designated Safeguarding Lead (DSL).
 - e. 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.

Policy Concerns

30. 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.
31. 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.
32. 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.
33. 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 Safeguarding and Child Protection policy.
34. I will report concerns about the welfare, safety, or behaviour of staff online to the Headteacher, in line with school Safeguarding and Child Protection policy and/or the Allegations Against staff policy.

Policy Compliance and Breaches

35. 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 and/or the Headteacher.
36. 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 children. 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.
37. 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.
38. I understand that if the school believes 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.
39. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with Barming Pre-School and Primary School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member:

Signed:

Date (DDMMYY).....

Wi-Fi Acceptable 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 education use only.
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 **Barming Pre-School and Primary School** Acceptable Use of Technology Policy (AUP) and School Behaviour and Exclusion policy 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 (**Miss H Rootes**) as soon as possible.
14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (**Miss H Rootes**) or the **Headteacher**.
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 have read, understood and agreed to comply with Barming Pre-School and Primary School Wi-Fi Acceptable Use Policy.

Name

Signed:Date (DDMMYY).....

Acceptable Use Policy (AUP) for Remote/Online Learning

Remote/Online Learning AUP Staff Statements

Barming Pre-School and Primary School Staff Remote/Online Learning AUP

The Remote/ Acceptable Use Policy (AUP) is in place to safeguarding all members of **Barming Pre-School and Primary 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 Office 365 Software and ClassDojo.
 - Microsoft Office 365 Software and ClassDojo have been assessed and approved by the **Headteacher**.
2. Staff will only use school managed or specific, 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 **Miss H Rootes**, the Designated Safeguarding Lead (DSL).
 - Staff will use work provided equipment unless approved by the Headteacher.
3. Online contact with pupils and/or parents/carers will not take place outside of the operating times as defined by SLT which are: 8am and 4pm.
4. All remote/online lessons will be formally timetabled; a member of SLT, DSL and/or Key Stage Leader is able to drop in at any time and must be sent the relevant links.
5. Live-streamed remote/online learning sessions will only be held with approval and agreement from the Headteacher/a member of SLT.

Data Protection and Security

1. Any personal data used by staff and captured by Microsoft Office 365 Software and ClassDojo when delivering remote learning will be processed and stored with appropriate consent.
2. All remote/online learning and any other online communication will take place in line with current school confidentiality expectations as outlined in our Trust Staff Code of Conduct.
3. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our policies.
4. Only members of Barming Pre-School and Primary School community will be given access to Microsoft Office 365 Software and ClassDojo.
5. Access to Microsoft Office 365 Software and ClassDojo will be managed in line with current IT security expectations as outlined in our Acceptable Use Policies.

Session management

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

7. Appropriate privacy and safety settings will be used to manage access and interactions. This includes disabling chats, keeping meeting IDs private, use of waiting rooms etc
8. When live streaming with pupils:
 - contact will be made via pupils email accounts and logins.
 - contact may also be made via a parents/carers account.
 - staff will mute/disable pupils' videos and microphones.
 - at least 2 members of staff will be present.
 - If this is not possible, SLT approval will be sought.
9. A pre-agreed invitation/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 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.
10. Alternative approaches and/or access will be provided to those who do not have access.

Behaviour expectations

11. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
12. 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.
 - Attendees may not record events for their own use.
13. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
14. 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.

15. 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

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

17. 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 SLT/Headteacher depending on what took place.

18. Inappropriate online behaviour will be responded to in line with existing policies such as Acceptable Use of Technology, Allegations against staff, Anti-bullying and School Behaviour and Exclusion Policy.

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

20. Any safeguarding concerns will be reported to **Miss H Rootes**, Designated Safeguarding Lead, in line with our Safeguarding and Child Protection policy.

I have read and understood the Barming Pre-School and Primary School Acceptable Use Policy (AUP) for remote/online learning.

Staff Member Name:

Date.....