Preston & Wingham Primary Schools Federation

Learning together, we grow kind hearts and healthy minds.

Acceptable Use Policy

APPROVAL & ADOPTION

This plan was formally agreed and adopted by the Governing Body on:

16th March 2026

Chair of Governors

Signed:

Staff Acceptable Use of Technology

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Preston & Wingham Primary Schools Federation 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 learners, 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 the federation's expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that federation 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.

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Preston & Wingham Primary Schools Federation both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies.

2. I understand that Preston & Wingham Primary Schools Federation Acceptable Use of Technology Policy (AUP) should be read and followed in line with the federation staff handbook.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the federation ethos, staff handbook and safeguarding policy, national and local education and child protection guidance, and the law.

Use of Preston & Wingham Primary Schools Federation Devices and Systems

4. I will only use the equipment and internet services provided to me by the federation, for example federation provided laptops, tablets and internet access for work purposes.

5. I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is not allowed unless by specific permission of the Executive Headteacher.

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 use a 'strong' password to access federation 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).*
    - I will protect the devices in my care from unapproved access or theft (e.g. *not leaving devices visible or unsupervised in public places).*

7. I will respect federation system security and will not disclose my password or security information to others.

8. 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.

9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager or Executive Headteacher.

10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR.

- 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 will be suitably protected. This may include data being encrypted by a method approved by the school.

11. 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.

12. I will not store any personal information on the federation 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.

13. I will ensure that federation 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.

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

15. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the IT System Manager and Executive Headteacher as soon as possible.

16. If I have lost any school related documents or files, I will report this to the IT System Manager, Executive Headteacher and federation Data Protection Officer as soon as possible.

17. Any images or videos of learners will only be used as stated in the federation image use policy.

- I understand images of learners must always be appropriate and should only be taken with school provided equipment and taken/published where learners and their parent/carer have given explicit consent.

Classroom Practice

18. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in the federation safeguarding, image use and online safety policies and the staff handbook.

19. I will promote online safety with the learners 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 learners feel comfortable to 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) as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
- make informed decisions to ensure any online safety resources used with learners is appropriate.

20. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the federation safeguarding policies.

21. 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.

Use of Social Media and Mobile Technology

22. I have read and understood the acceptable use of social media and mobile technology policy which covers expectations regarding staff use of mobile technology and social media.

23. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role and in line with the staff handbook when using school and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.

- I will take appropriate steps to protect myself online when using social media as outlined in the social media and mobile technology section within this policy.
- I am aware of the school expectations with regards to use of personal devices and mobile technology, including mobile phones as outlined in the social media and mobile technology acceptable use policy.
- I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.
- I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the federation staff handbook and the law.

24. My electronic communications with current and past learners 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 learners, 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 learners and/or parents/carers.
- If I am approached online by a learner or parents/carer, I will not respond and will report the communication to the Designated Safeguarding Lead (DSL).
- Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSL

25. 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.

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 is 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 federation into disrepute.

Policy Compliance

29. I understand that the federation may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

Policy Breaches or Concerns

30. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the federation safeguarding policy.

31. I will report concerns about the welfare, safety, or behaviour of staff to the Executive Headteacher, in line with the allegations against staff policy.

32. I understand that if the school believe that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the disciplinary policy.

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

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

Visitor and Volunteer Acceptable Use of Technology

As a professional organisation with responsibility for children's safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of their professional responsibilities when using technology. This AUP will help Preston & Wingham Primary Schools Federation ensure that all visitors and volunteers understand the federation's expectations regarding safe and responsible technology use.

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services provided to me or accessed as part of my role within Preston/Wingham Primary School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning systems and communication technologies.

2. I understand that Preston & Wingham Primary Schools Federation AUP should be read and followed in line with the staff handbook.

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 federation ethos, staff handbook and safeguarding policies, national and local education and child protection guidance, and the law.

Data and Image Use

4. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.

5. I understand that I am not allowed to take images or videos of learners on my personal devices. Any images or videos of learners will only be taken in line with the federation's image use policy.

Classroom Practice

6. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of learners.

7. I will support staff in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the children in my care.

8. I will immediately report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) in line with the federation safeguarding policy.

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

Use of Social Media and Mobile Technology

10. I have read and understood the acceptable use of social media and mobile technology policy which covers expectations regarding staff use of social media and mobile technology.

11. I will ensure that my online reputation and use of technology and is compatible with my role within the school. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
    - I will take appropriate steps to protect myself online as outlined in the online safety/social media policy.
    - I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.
    - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the federation staff handbook and the law.

12. My electronic communications with learners, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via school approved communication channels such as via a school provided email address, account or telephone number.
    - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the DSL.

13. 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 Designated Safeguarding Lead.

14. 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.

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

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

Policy Compliance, Breaches or Concerns

17. I understand that the school may exercise its right to monitor the use of school information systems, including internet access and the interception of emails, to monitor policy compliance and

to ensure the safety of learners, staff and visitors/volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

18. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the Designated Safeguarding Lead in line with the federation safeguarding policy.

19. I will report concerns about the welfare, safety, or behaviour of staff to the executive headteacher, in line with the allegations against staff policy.

20. I understand that if the school believes that if unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.

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

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the federation community are fully aware of the federation boundaries and requirements when using the federation 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 federation community are reminded that technology use should be consistent with our ethos, other appropriate policies, and the law.

1. The federation provides Wi-Fi for the school community and allows access for educational purposes only.

2. I am aware that the federation will not be liable for any damages or claims of any kind arising from the use of the wireless service. The federation 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 Preston & Wingham Primary Schools Federation Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy which all learners/staff/visitors and volunteers must agree to and comply with.

4. The federation 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 federation 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 federation 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 federation 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 federation 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 federation into disrepute.

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

14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead.

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 federation suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the federation may terminate or restrict usage. If the federation 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.

Remote Learning Acceptable Use

The Remote Learning Acceptable Use protocol is in place to safeguarding all members of Preston & Wingham Primary Schools Federation community when taking part in remote learning following any full or partial school closures.

Leadership Oversight and Approval

1. Remote learning will only take place using Microsoft 365 Education.

- Microsoft 365 Education has been assessed and approved by the DfE, the governing body, the Senior Leadership Team (SLT) and our technical support.

2. Staff will only use school managed accounts with learners and/or parents/carers.
    - Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
    - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with Designated Safeguarding Lead (DSL).
    - Staff will use work provided equipment where possible e.g. a school laptop, tablet, or other mobile device.
3. Online contact with learners and/or parents/carers will not take place outside of the usual school day (9.00 – 3.30).
4. All remote lessons will be formally timetabled; a member of SLT is able to drop in at any time.
5. Live streamed remote learning sessions will only be held with approval and agreement from a member of SLT.

Data Protection and Security

6. Any personal data used by staff and captured by Microsoft 365 Education when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
7. All remote learning and any other online communication will take place in line with current federation confidentiality expectations.
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 Preston & Wingham Primary Schools Federation community will be given access to Microsoft 365 Education.
10. Access to Microsoft 365 Education will be managed in line with current IT security expectations as outlined in our acceptable use policy.

Session Management

11. Staff will record the length, time, date, and attendance of any sessions held. This record will be sent to the school office.
12. Appropriate privacy and safety settings will be used to manage access and interactions.
13. When live streaming with learners:
    - contact will be made via learners' school provided email accounts and/or logins.
    - staff will mute/disable learners' videos and microphones and will unmute/disable when appropriate to do so.
    - SLT approval will be sought.
14. Live 1 to 1 sessions will not take place.
15. 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.
    - Learners and/or parents/carers should not forward or share access links.
    - If learners/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
    - Learners 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.
16. Alternative approaches will be provided to those who do not have access.

Behaviour Expectations

17. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
18. All participants are expected to behave in line with existing school policies and expectations.
19. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
20. 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.
21. 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

22. Participants are encouraged to report concerns during remote and/or live streamed sessions to the member of staff running the session.
23. 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 Head of School.
24. 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.
25. Sanctions for deliberate misuse may include, for example, restricting/removing use, contacting police if a criminal offence has been committed.
26. Any safeguarding concerns will be reported to the Designated Safeguarding Lead, in line with our safeguarding policy.

Mobile Technology and Social Media

Expectations

Preston & Wingham Primary Schools Federation recognises that personal communication through mobile technologies is part of everyday life for many learners, staff and parents/carers. Mobile technology needs to be used safely and appropriately within the setting.

All use of mobile technology, including mobile phones and personal devices such as tablets, e-readers, games consoles and wearable technology (such as 'smart watches' and fitness trackers which facilitate communication or have the capability to record sound or imagery), will take place in accordance with our policies, such as behaviour, safeguarding, acceptable use, image use, the staff handbook and with the law.

Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of our federation community are advised to:

- take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.

- use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared

Mobile phones and personal devices are not permitted to be used in specific areas on site, such as the toilets.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our behaviour policies.

All members of the federation community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or safeguarding policies.

Staff use of personal devices and mobile phones

Members of staff will ensure that use of any personal phones and mobile devices will take place in accordance with the law, as well as relevant policy and procedures, such as confidentiality, safeguarding, data security and acceptable use of technology.

Staff will be advised to:

- keep mobile phones and personal devices in a safe and secure place during lesson time.
- keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson time.
- ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
- not use personal devices during teaching periods unless written permission has been given by a member of SLT such as in emergency circumstances.
- ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers. Any pre-existing relationships which could undermine this, will be discussed with the DSL.

Staff will only use *school* provided equipment (not personal devices):

- to take photos or videos of learners in line with our image use policy.
- to work directly with learners during lessons/educational activities.
- to communicate with parents and carers.

If a member of staff breaches our policy, action will be taken in line with our staff behaviour and allegations policy.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence using a personal device or mobile phone, the police will be

contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

Learners use of personal devices and mobile phones

Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

The federation expects learners' personal devices and mobile phones to be handed to the class teacher on arrival at school who will keep them *in a secure place until the end of the school day.*

Mobile phones or personal devices will not be used on site by learners unless as part of an approved and directed curriculum-based activity with consent from the head of school.

If a learner requires access to a personal device in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the *head of school p*rior to use being permitted. Any arrangements regarding access to personal devices in exceptional circumstances will be documented and recorded by the *school*.

Where learners' mobile phones or personal devices are used when learning at home, such as in response to local or full lockdowns, this will be in accordance with our *Acceptable Use Policy*.

Any concerns regarding learners use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including safeguarding and behaviour. Appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy. Concerns regarding policy breaches by learners will be shared with parents/carers as appropriate.If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Visitors' use of personal devices and mobile phones

Parents/carers and visitors, including volunteers and contractors, should ensure that mobile phones are on silent and are not used in school unless an approved member of staff gives permission.

Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our acceptable use of technology policy and other associated policies, including but not limited to behaviour, safeguarding and image use.

Members of staff are expected to challenge visitors if they have concerns and inform the DSL (or deputy) or *head of school* of any breaches of our policy.

Officially provided mobile phones and devices

Staff providing formal remote learning will do so using *school* provided equipment in accordance with our *acceptable use policy.*

School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff and/or pupils.

Where staff or pupils are using *school* provided mobile phones and/or devices, they will be informed prior to use that activity may be monitored for safeguarding reasons and to ensure policy compliance.

School mobile phones and devices will always be used in accordance with the acceptable use of technology policy and other relevant policies.

Acceptable Use by Pupils

Through computing lessons and the wider curriculum all pupils will be taught:

- to only use the internet when an adult is present
- to only click on links and buttons when they know what they do
- to keep their personal information and passwords safe online
- to only send messages online which are polite and friendly
- that the school can see what they are doing online at all times
- If they see anything online that they shouldn't or that makes them feel worried or upset then they will minimise the page and tell an adult straight away
- that they can visit www.thinkuknow.co.uk (include other appropriate links) to learn more about keeping safe online
- to know that not everything or everyone online is honest or truthful
- to know that AI can distort or change the truth (fake news and images)
- that they must not access or change other people's files or information
- that they can only change the settings on the computer if a teacher/technician has allowed them to
- that people they meet online may not always be who they say they are. If someone online suggests meeting up, they must immediately talk to an adult
- that If they are aware of anyone being unsafe with technology then they will report it to a teacher
- that remote learning will only take place using Microsoft Classrooms and during usual school times.
- That they will only use their school provided email accounts and/or login to access remote learning, that they will not share their login/password with others and they will not share any access links to remote learning sessions with others.
- That when taking part in remote learning they will behave as they would in the classroom including wearing appropriate clothing and being in a suitable location. They will attend lessons in a shared/communal space or room with an open door and/or where possible when they can be supervised by a parent/carer or another appropriate adult.