Acceptable Use of Technology Policy for

Educational Settings

2021-22

**Version 1**

**Published August 2021**

**Early Years and Key Stage 1 (0-6)**

I understand that Five Wents Pre-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 links and buttons online when I know what they do.
* I keep my personal information and passwords safe.
* I only send messages online which are polite and friendly.
* I always tell an adult if something online makes me feel upset, unhappy, or worried.
* I can visit [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) to learn more about keeping safe online.
* I know that if I do not follow the rules:
* An adult will talk to me about how I can keep myself safe
* An adult will discuss it with my parents/carers
* I have read and talked about these rules with my parents/carers.

**Shortened version**

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

**Acceptable Use of Technology for Parents/Carers**

**Parent/Carer AUP Suggestions**

***We suggest that these points should be adhered to in order to keep you and your child safe whilst using technology***

Five Wents Pre-School **Learner Acceptable Use of Technology Policy Acknowledgment**

1. I, with my child, have read and discussed Five Wents Pre-School learner acceptable use of technology policy (AUP) and understand that the AUP will help keep my child safe online.
2. I understand that the AUP applies to my child use of systems at home, and personal use where there are safeguarding and/or behaviour concerns.
3. I am aware that any use of Five Wents Pre-School systems may be monitored for safety and security reason 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.
4. I understand that my child needs a safe and appropriate place to access remote learning if Five Wents Pre-School is closed for any reason, including Covid-19. I will ensure my child’s access to remote learning is appropriately supervised and any use is in accordance with the setting remote learning AUP.
5. I understand that the setting will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe using suggested websites whilst at home. I understand that the setting cannot ultimately be held responsible for the nature and content of materials accessed on the internet or if my child is using mobile technologies.
6. I and my child, are aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the setting community.
7. I understand that the setting will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child’s safety online.
8. I will inform the setting (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 setting community’s safety online.
9. 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 setting.
10. I will support the setting online safety approaches. I will use appropriate parental controls and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

**Staff and Volunteer Acceptable Use of Technology Policy**

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Five Wents Pre-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 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 Five Wents Pre-School expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that Five Wents Pre-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 AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Five Wents Pre-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 and online and offline communication technologies**.**
2. I understand that Five Wents Pre-School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the setting staff behaviour policy/code of conduct.
3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the setting ethos, setting staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

**Use of Setting** **Devices and Systems**

1. I will only use the equipment and internet services provided to me by the setting for example setting provided laptops, tablets, mobile phones, and internet access, when working with learners.
2. I understand that any equipment and internet services provided by my workplace is intended for education purposes and 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.
3. Where I deliver or support remote learning, I will comply with the setting remote learning AUP.

**Data and System Security**

1. 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 setting 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, for example not leaving devices visible or unsupervised in public places.*
2. I will respect setting system security and will not disclose my password or security information to others.
3. 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 manager.
4. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the manager.
5. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the setting 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 setting 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 setting.
6. I will not keep documents which contain setting 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, upload any work documents and files in a password protected environment.
7. I will not store any personal information on the setting IT system, including setting laptops or similar device issued to members of staff, that is unrelated to setting activities, such as personal photographs, files or financial information.
8. I will ensure that setting 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.
9. I will not attempt to bypass any filtering and/or security systems put in place by the setting.
10. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the Manager as soon as possible.
11. If I have lost any setting related documents or files, I will report this to the Manager/Data Protection Officer, Sasha Tadman, as soon as possible.
12. Any images or videos of learners will only be used as stated in the setting camera and image use policy. I understand images of learners must always be appropriate and should only be taken with setting provided equipment and only be taken/published where learners and/or parent/carers have given explicit written consent.

**Classroom Practice**

1. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces.
2. I have read and understood the setting mobile technology and social media policies.
3. 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 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) (Candice Graham) or a deputy (Sasha Tadman) 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.
4. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the setting child protection policies.
5. 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**

1. 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 behaviour policy/code of conduct and the setting mobile technology policy and the law.

**Online Communication, including Use of Social Media**

1. 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 staff behaviour policy/code of conduct, the setting social media policy and the law. In line with the setting social media policy:
   * I will take appropriate steps to protect myself and my reputation online when using communication technology, including the use of social media as outlined in the social media policy (can be found on www.fivewentspreschool.co.uk).
   * I will not discuss or share data or information relating to learners, staff, setting business or parents/carers on social media.
2. 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 setting approved and/or provided communication channels and systems, such as a setting 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 their parents/carers.
   * If I am approached online by a current or past learner or parents/carer, I will not respond and will report the communication to my line manager and (Sasha Tadman) 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 and/or manager.

**Policy Concerns**

1. 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.
2. 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.
3. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the setting into disrepute.
4. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the setting child protection policy.
5. I will report concerns about the welfare, safety, or behaviour of staff to the manager, in line with the allegations against staff policy.

**Policy Compliance and Breaches**

1. If I have any queries or questions regarding safe and professional practise online either in setting or off site, I will raise them with the DSL and the manager.
2. I understand that the setting may exercise its right to monitor the use of its 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.
3. I understand that if the setting believe that unauthorised and/or inappropriate use of setting systems or devices is taking place, the setting may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.
4. I understand that if the setting believe that unprofessional or inappropriate online activity, including behaviour which could bring the setting into disrepute, is taking place online, the setting may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.
5. I understand that if the setting suspects criminal offences have occurred, the police will be informed.

**I have read, understood and agreed to comply with Five Wents Pre-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 Use Policy**

***For those using setting provided Wi-Fi. Settings may wish to use a paper or electronic AUP for guest access of Wi-Fi by members of the community. This template is provided for settings to adapt and use as appropriate.***

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

1. The setting provides Wi-Fi for the setting community and allows access for uploading observations and researching provocations.
2. I am aware that the setting will not be liable for any damages or claims of any kind arising from the use of the wireless service. The setting takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the setting premises that is not the property of the setting.
3. The use of technology falls under setting Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy such as data security, safeguarding/child protection which all learners/staff/visitors and volunteers must agree to and comply with.
4. The setting 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. The setting 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 setting service is adequately secure, such as up-to-date anti-virus software, systems updates.
7. The setting wireless service is not secure, and the setting cannot guarantee the safety of traffic across it. Use of the setting 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 setting accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the setting 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 setting 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 setting security and filtering systems or download any unauthorised software or applications.
11. My use of setting Wi-Fi will be safe and responsible and will always be in accordance with the setting 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 setting into disrepute.
13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Candice Graham) as soon as possible.
14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (Candice Graham) or the manager.
15. I understand that my use of the setting Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation*.* If the setting suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the setting may terminate or restrict usage. If the setting 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 Five Wents Pre-School Wi-Fi acceptable Use Policy.**

Name ……………………………………………………………………………………………………..…...

Signed: ………………………........................................................Date (DDMMYY)……………………..