Child Acceptable Use of Technology Statements

Early Years and Key Stage 1 (0-6)

- I understand that the nursery and out of school club Acceptable Use Policy will help keep me safe and happy online.
- I only use the internet when an adult is with me.
- I only click on online links and buttons when I know what they do. If I am not sure, I ask an adult first.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know the setting can see what I am doing online when I use setting computers or tablets.
- I always tell a member of staff if something online makes me feel upset, unhappy, or worried.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
- I know that if I do not follow the setting rules my permission to use the device will be revoked and my parents may be informed.
- I have read and talked about these rules with my parents/carers.

Shortened KS1 version (for use on posters or with very young children)

- 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.

Key Stage 2 (7-11)

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

Safe

- I will behave online the same way as I behave in the classroom.
- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are safe and appropriate, and if I have permission.
- I only talk with, and open messages, from people I know.
- I will only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

Learning

- I ask the out of school club manager before using my own personal smart devices and/or mobile phone at out of school club.

- I always ask permission from an adult before using the internet.
- I only use websites and search engines that a member of out of school club staff has chosen.
- I use out of school club devices for school work unless I have permission otherwise.

Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on various sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, images, or text I use.

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 minimise the screen, shut the laptop lid or turn off the screen and tell an adult immediately.
- If I am aware of anyone being unsafe with technology, I will report it to a staff member at out of school club.
- I know it is not my fault if I see, or someone sends me, something upsetting or unkind online.
- I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.

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 out of school club owned devices and networks are monitored to help keep me safe. This means someone at the setting may be able to see and/or check my online activity when I use setting devices and/or networks if they are concerned about my or anyone else's safety or behaviour.
- If, for any reason, I need to bring a personal device, for example a smart/mobile phone and/or other wearable technology into setting then will ask my parent and out of school club staff member for permission to use it. If I don't have permission to use it, I know that it is to be handed in to the office and then collected at the end of the setting day.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online or to see help.
- I know that if I do not follow the setting rules then I may not be allowed to use devices at out of school club.

Shortened KS2 version (for use on posters)

- I ask an adult about which websites I can use.
- I will not assume information online is true.
- I know there are laws that stop me copying online content.
- I know I must only open online messages that are safe. If I am unsure, I will not open it without speaking to an adult first.
- I know that people online are strangers, and they may not always be who they say they are.
- If someone online suggests meeting up, I will always talk to an adult straight away.
- I will not use technology to be unkind to people.
- I will keep information about me and my passwords private.
- I always talk to an adult if I see something which makes me feel worried.
- I know my use of setting devices and systems can be monitored.

Acceptable Use of Technology for Staff, Visitors and Volunteers Statements

Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Hythe Bay 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 children, 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 Hythe Bay expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that setting 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 setting or accessed by me as part of my role within Hythe Bay, 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 and communication technologies**.**

2. I understand that Hythe Bay's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the child protection policy and 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

4. 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 at the setting, unless I am in the staff room.

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 only allowed with the manager's permission and can be revoked at any time.

Data and system security

6. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
    - I will use a ‘strong’ password to access setting systems.
    - I will protect the devices in my care from unapproved access or theft, for example not leaving devices visible or unsupervised in public places.

7. I will respect setting 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.

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

11. 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, I will use the setting network to upload any work documents and files in a password protected environment.

12. 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.

13. 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.

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

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 ICT Support Provider as soon as possible.

16. If I have lost any setting related documents or files, I will report this to the ICT Support Provider and setting Data Protection Officer as soon as possible.

17. Any images or videos of children will only be used as stated in the setting policies and parent consent forms. I understand images of children must always be appropriate and should only be taken with setting provided equipment and only be taken/published where children and/or parent/carers have given explicit written consent.

Classroom practice

18. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by Hythe Bay as detailed in policies, and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.

19. 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, in line with the setting child protection policy.

20. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in policies.

21. 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:
    - 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 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.
    - involving the Designated Safeguarding Lead (DSL) or a deputy 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.
    - Informing the DSL and/or leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
    - make informed decisions to ensure any online safety resources used with children is appropriate.

22. 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

23. I have read and understood the setting mobile and smart technology and social media policies which addresses use by children and staff.

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

Online communication, including use of social media

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

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

27. My electronic communications with current and past children 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 children, 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 children and/or their parents/carers.
    - If I am approached online by a current or past children or parents/carers, I will not respond and will report the communication to my line manager and Designated Safeguarding Lead (DSL).
    - Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL and/or manager.

Policy concerns

28. 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.

29. 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.

30. 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.

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

32. I will report concerns about the welfare, safety, or behaviour of staff online to the manager, in line with setting child protection policy and/or the allegations against staff policy.

Policy Compliance and Breaches

33. 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/or the manager.

34. I understand that the setting may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of children and staff. This includes monitoring all setting provided devices and setting systems and networks including setting provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via setting 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.

35. I understand that if the setting believe that unauthorised and/or inappropriate use of setting devices, systems or networks is taking place, the setting may invoke its disciplinary procedures as outlined in the code of conduct.

36. 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 code of conduct.

37. 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 Hythe Bay Children’s Centre’s 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)……………………………………………………………………….……...

Visitor and Volunteer Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of our behaviour expectations and their professional responsibilities when using technology. This AUP will help Hythe Bay Children's Centre ensure that all visitors and volunteers understand the setting's expectations regarding safe and responsible technology use.

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 setting or accessed by me as part of my role within Hythe Bay, professionally and personally. 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 and communication technologies**.**

2. I understand that AUP should be read and followed in line with the setting code of conduct.

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 setting ethos, setting policies, national and local education and child protection guidance, and the law.

4. 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.

5. 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.

6. 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.

Data and image use

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

8. I understand that I am not allowed to take images or videos of children without explicit consent from the manager and the children's parents. Any images or videos of children will only be taken in line with the setting policies.

Classroom practice

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

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

11. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the setting community, I will report this to the DSL and IT provider, in line with the setting child protection policy.

12. 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 mobile devices and smart technology

13. In line with the setting mobile and smart technology policy, I understand that mobile phones and personal devices are not permitted or are only permitted within the staffroom or nursery office when no children are present.

Online communication, including the use of social media

14. I will ensure that my online reputation and use of technology and is compatible with my role within the setting. 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 setting policies.
    - I will not discuss or share data or information relating to children, staff, setting 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 setting code of conduct and the law.

15. My electronic communications with children, 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 setting approved communication channels such as via a setting 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 my ability to comply with this will be discussed with the DSL and/or manager.

Policy compliance, breaches or concerns

16. If I have any queries or questions regarding safe and professional practice online either in setting or off site, I will raise them with the Designated Safeguarding Lead and/or the manager.

17. I understand that the setting may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of children and staff. This includes monitoring all setting provided devices and setting systems and networks including setting provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via setting 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.

18. I will report and record concerns about the welfare, safety or behaviour of children or parents/carers online to the Designated Safeguarding Lead in line with the setting child protection policy.

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

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

21. 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 Hythe Bay Children's Centre visitor/volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer: ………………………………………………………………...……………

Signed: ………………………...

Date (DDMMYY)……………………………………...

Wi-Fi Acceptable Use Policy

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 school provides Wi-Fi for the setting community and allows access for education and professional purposes.

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 Hythe Bay Acceptable Use of Technology Policy (AUP), which all out of school club children, 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 setting service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The school cannot guarantee the safety of traffic across the wireless service. 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 setting 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 and 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 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 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 as soon as possible.

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

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 or setting 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 or 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 Hythe Bay Children's Centre Wi-Fi Acceptable Use Policy.

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

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