Hythe Bay Children's Centre

Acceptable Use of Technology Policy

September 2021

Contents

Learner Acceptable Use of Technology Statements

Although statements for learners are collected within key stages, it is recommended that settings amend and adapt them according to their own cohorts needs.

The statements and headers are suggestions only and some statements are duplicated; we encourage educational settings to work with learners to amend the statements so they can develop ownership and understanding of the expectations.

Early Years and Key Stage 1 (0-6)

I understand that the setting 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 know the setting can see what I am doing online when I use setting computers and tablets.
- I always tell an adult if something online makes me feel upset, unhappy, or worried.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
- I have read and talked about these rules with an adult.

Shortened KS1 version (e.g. for use on posters)

- 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 setting Acceptable Use Policy will help keep me safe and happy online at home and at setting.

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 my teacher before using my own personal smart devices and/or mobile phone at the setting.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use setting devices 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.

Understand

- I understand that the setting internet filter is there to protect me, and I will not try to bypass it.
- I know that all setting devices and systems are monitored to help keep me safe, including when I use them at home.
- 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.

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page, close the laptop lid or turn off my screen, and tell an adult straight away.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher.
- I know it is not my fault if I see, or someone sends me, something bad 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.

Acceptable Use of Technology Statements and Forms for Parents/Carers

Parent/Carer AUP Acknowledgement

Hythe Bay Children's centre Learner Acceptable Use of Technology Policy Acknowledgment

1. I, with my child, have read and discussed the 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 setting devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns.

3. I am aware that any use of setting devices and 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 am aware that the setting mobile/smart technology policy states that my child can use a personal device and mobile/smart technology on site only with a teacher's permission.

5. I understand that the setting will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use setting devices and systems. 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 by 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.

Sample Parent/Carer Acceptable Use of Technology Policy

1. I know that my child will be provided with internet access and will use a range of IT systems including in order to access the curriculum and be prepared for modern life whilst at Hythe Bay Children's Centre.

2. I am aware that learners use of mobile technology and devices, such as mobile phones, may be permitted by a teacher.

3. I am aware that any internet and technology use using setting equipment may be monitored for safety and security reasons, to safeguard both my child and the setting systems. This monitoring will take place in accordance with data protection (including GDPR) and human rights legislation.

4. I understand that the setting will take every reasonable precaution, including monitoring and filtering systems, to ensure that learners are safe when they use the setting internet and systems. I understand that the setting cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

5. 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 setting.

6. I have read and discussed the learner Acceptable Use of Technology Policy (AUP) with my child.

7. I will support setting safeguarding policies and will ensure that I appropriately monitor my child's use of the internet outside of setting and discuss online safety with them when they access technology at home.

8. I know I can seek support from the setting about online safety, such as via the setting website, to help keep my child safe online at home.

9. I will support the setting approach to online safety. I will role model safe and positive online behaviour for my child by sharing images, text, and video online responsibly.

10. I, together with my child, 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.

11. I understand that a partnership approach to online safety is required. If the setting has any concerns about either my or my child's behaviour or safety online, then I will be contacted.

12. I understand that if I or my child do not abide by the Hythe Bay Children's Centre AUP, appropriate action will be taken. This could include sanctions being applied in line with the setting policies (list as appropriate) and if a criminal offence has been committed, the police being contacted.

13. I know that I can speak to the Designated Safeguarding Lead, my child's teacher or the manager if I have any concerns about online safety.

Acceptable Use of Technology for Staff, Visitors and Volunteers Statements

Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Hythe Bay Children's Centre's 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 Hythe Bay Children's Centre's 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 AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Hythe Bay Children's Centre 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 Hythe Bay Children's Centre Acceptable Use of Technology Policy (AUP) should be read and followed in line with the setting staff behaviour 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 working with learners.

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 only when permitted by the setting manager or a trustee.

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 by 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 GDPR in line with the setting information security procedures.

    - 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 learning platform to upload any work documents and files in a password protected environment or setting approved/provided VPN.

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 learners will only be used as and when consent is obtained from their parent in writing. 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

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 relevant policies and procedures e.g. child protection, online safety.

19. I have read and understood the setting mobile technology and social media policies.

20. 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) or a deputy 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.

21. 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.

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

Online Communication, including Use of Social Media

24. 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 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.
- I will not discuss or share data or information relating to learners, staff, setting business or parents/carers on social media.

25. 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 learners and/or their parents/carers.
- If I am approached online by a current learner or parents/carer, 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 will be discussed with the DSL and/or manager.

Policy Concerns

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

27. I will not attempt to access, create, transmit, display, publish or forward any material or content online that 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 setting into disrepute.

29. 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.

30. 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

31. 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.

32. 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.

33. I understand that if the setting believes 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 code of conduct.

34. I understand that if the setting believes 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.

35. 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 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 settings 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 provided to me or accessed as part of my role within Hythe Bay Children's Centre, 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 Hythe Bay Children's Centre AUP should be read and followed in line with the setting staff 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 staff behaviour 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.

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 setting child protection 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 Mobile Devices and Smart Technology

10. In line with the setting mobile technology policy, I understand that mobile phones and personal devices are not permitted in the rooms with children.

Online Communication, including the Use of Social Media

11. 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 online safety/social media policy
    - I will not discuss or share data or information relating to learners, 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.

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 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 this will be discussed with the DSL and/or manager.

Policy Compliance, Breaches or Concerns

13. 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.

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 setting into disrepute.

17. I understand that the setting may exercise its right to monitor the use of setting 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 setting child protection policy.

19. I will report concerns about the welfare, safety, or behaviour of staff 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's 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 setting provides Wi-Fi for the setting community and allows access for (state purpose, for example education use only). Settings should include any include information about time limits, passwords, and security.

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 the Acceptable Use of Technology Policy (AUP) and online safety procedure 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. 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 may not be 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 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 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 Hythe Bay Children's Centre's Wi-Fi acceptable Use Policy.

Name ……..…...

Signed: ……..Date (DDMMYY)……...

Acceptable Use Policy (AUP) for Remote Learning

Further information and guidance regarding remote learning:

- Local guidance:
  - Kelsi:
    - Guidance for Full Opening in September
    - Online Safety Guidance for the Full Opening of Schools
  - The Education People: Covid-19 Specific Safeguarding Guidance and Resources
    - 'Safer remote learning during Covid-19: Information for School Leaders and DSLs'
    -

- National guidance:
  - DfE:
    - 'Safeguarding and remote education during coronavirus (COVID-19)
  - SWGfL:
    - Safer Remote Learning
  - LGfL: Coronavirus Safeguarding Guidance
  - NSPCC:
    - Undertaking remote teaching safely
  - Safer Recruitment Consortium:
    - 'Guidance for safer working practice for those working with children and young people in education settings Addendum' April 2020

Remote Learning AUP - Staff Statements

Hythe Bay Children's Centre's Staff Remote Learning AUP

The Remote Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of Hythe Bay Children's Centre's community when taking part in remote learning following any full or partial setting closures.

Leadership Oversight and Approval

1. Remote learning will only take place using Connect Childcare.
    - Connect Childcare has been assessed and approved by the trustees.
2. Staff will only use setting managed or specific, approved professional 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 the Designated Safeguarding Lead (DSL).
    - Staff will use work provided equipment where possible e.g. a setting laptop, tablet, or other mobile device.
3. Online contact with learners and/or parents/carers will not take place outside of the operating times: 7:30am and 6:30pm.
4. Live-streamed remote learning sessions will only be held with approval and agreement from a member of the management team.

Data Protection and Security

5. Any personal data used by staff and captured by Connect Childcare or Zoom when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
6. All remote learning and any other online communication will take place in line with current setting confidentiality expectations as outlined in setting procedures.
7. All participants will be made aware that Connect Childcare records activity.
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 the setting community will be given access to Connect Childcare or Zoom.
10. Access to Connect Childcare or Zoom will be managed in line with current IT security expectations as outlined in setting policies and procedures.

Session Management

11. Staff will record the length, time, date, and attendance of any sessions held.
12. Appropriate privacy and safety settings will be used to manage access and interactions.
    - contact will be made via a parents/carer's account.
    - at least 2 members of staff will be present.
13. 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.

14. Alternative approaches and/or access will be provided to those who do not have access.

Behaviour Expectations

15. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
16. All participants are expected to behave in line with existing setting policies and expectations. This includes:
    - Appropriate language will be used by all attendees.
    - Staff, children and parents will not take or record images for their own personal use.
    - Setting decisions about if other attendees can or cannot record events for their own use, and if so, any expectations or restrictions about onward sharing.
17. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
18. 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.
19. 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

20. Participants are encouraged to report concerns during remote and/or live-streamed sessions, for example via:
    - reporting concerns to the member of staff running the session, telling a parent/carer, telling a staff member.
21. 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 Designated Safeguarding Lead and/or manager.
22. 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.
23. Sanctions for deliberate misuse may include: restricting/removing use, contacting police if a criminal offence has been committed.
24. Any safeguarding concerns will be reported to the Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the Hythe Bay Children's Centre Acceptable Use Policy (AUP) for remote learning.

Staff Member Name: ……

Date……