Acceptable Use of Technology Policy For Birchwood

Adopted by Birchwood from the Education People - September 2021
Approved by the Management Committee – September 2021
Review date – September 2022

Contents

Using the AUP Templates: Guidance Notes

Education leaders should ensure their policies and procedures are in line with statutory requirements. 'Keeping Children Safe in Education' (KCSIE) 2021 states that schools and colleges should have a '*staff behaviour policy (sometimes called the code of conduct) which should, amongst other things, include acceptable use of technologies, staff/pupil relationships and communications including the use of social media*'.

This document will support educational settings in creating Acceptable Use Policies (AUP) which are relevant to their communities and reflects the needs and abilities of learners and technology available.

Leaders, managers, and DSLs should adapt the content to include specific local information such named points of contact, as well as specific procedures and expectations. These decisions and details will vary from setting to setting, so this template should be used as a starting framework. It will not be appropriate for educational settings to adopt the templates in their entirety; DSLs and leaders should ensure unnecessary content is removed.

Key Points

- AUPs should be recognised by educational settings as part of the portfolio of safeguarding policies and as part of the settings code of conduct and/or behaviour policies.
- AUPs are not technical policies and as such should fall within the role and responsibilities of the Designated Safeguarding Lead (DSL) with approval from SLT.
    - The DSL is likely to require advice and support from other staff within the setting to ensure the AUP is robust and accurate, for example technical staff, therefore leaders should ensure that time is allocated to ensure this takes place.
- Where possible and appropriate, learners, staff and parents/carers should be directly involved in the creation and updating of AUPs.
- AUPs should be reviewed on an at least annual basis and updated following any substantial policy or technology changes locally or nationally; this will be especially important following closures in respond to the Covid-19 pandemic.
- Leaders should consider how they evidence that all members of the community have read and understood policies e.g. keeping copies of signed agreements, publishing AUPs on the school/setting website/intranet.
- Educational settings should ensure AUPs are individualised for their specific context; settings will need to adapt the templates in line with their own technology use, for example the expectations or requirements may vary if settings use laptops or tablets.

Disclaimer

The Education People make every effort to ensure that the information in this document is accurate and up to date. If errors are brought to our attention, we will correct them as soon as practicable.

Learner Acceptable Use of Technology Sample 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 template statements and headers are suggestions only and some statements are duplicated; we encourage educational settings to work with learners and amend them to develop ownership and understanding.

Key Stage 3/4/5 (11-18)

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

- I know that Birchwood computers, tablets, laptops, and internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I am not sure if something is allowed, I will ask a member of staff.
- I know that my use of Birchwood computers and devices, systems and on-site internet access will be monitored to keep me safe and ensure policy compliance.
- I will keep my password safe and private as my privacy, Birchwood work and safety must be protected.
- If I need to learn online at home, I will follow the Birchwood remote learning AUP
- I will write emails and online messages carefully and politely as I know they could be forwarded or seen by someone I did not intend.
- I will only use social media sites with permission and at the times that are allowed.
- I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place, with a trusted adult present.
- I know that bullying in any form (on and offline) is not tolerated and I know that technology should not be used for harassment.
- I 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 Birchwood community.
- I understand that it may be a criminal offence or breach of the Birchwood policy to download or share inappropriate pictures, videos, or other material online. I also understand that it is against the law to take, save or send indecent images of anyone under the age of 18.
- I will protect my personal information online.
- I will not access or change other people files, accounts, or information.
- I will only upload appropriate pictures or videos of others online and when I have permission.
- I will only use my personal device/mobile phone in Birchwood if I have permission from a teacher.
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources.
- I will always check that any information I use online is reliable and accurate.

- I will make sure that my internet use is safe and legal, and I am aware that online actions have offline consequences.
- I will only change the settings on the computer if a teacher has allowed me to.
- I know that use of the Birchwood ICT system for personal financial gain, gambling, political purposes, or advertising is not allowed.
- I understand that the Birchwood internet filter is there to protect me, and I will not try to bypass it.
- I know that if Birchwood suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices.
- I know that if I do not follow the Birchwood AUP then:
    - ***I could lose my access to the School computer/laptop***
    - ***My Parents/Carers will be informed***
    - ***I could be excluded from Birchwood***
    - ***I may be reported to the Police of online safety organisations for misuse.***
- If I am aware of anyone trying to misuse technology, I will report it to a member of staff.
- I will speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared, or uncomfortable.
- I will visit www.thinkuknow.co.uk www.childnet.com and www.childline.org.uk to find out more about keeping safe online.
- I have read and talked about these rules with my parents/carers.

Alternative KS3/4 Statements

Learning

- I know that Birchwood computers, devices and internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I am not sure if something is allowed, I will ask a member of staff.
- If I need to learn online at home, I will follow the Birchwood remote learning AUP.
- I will only use my personal device/mobile phone in Birchwood if I have permission from a teacher.

Safe

- I will make sure that my internet use is safe and legal, and I am aware that online actions have offline consequences.
- I know that my use of Birchwood devices and systems will be monitored, at home and at school, to protect me and to ensure I comply with the acceptable use policy.
- I know that people online are not always who they say they are and that I must always talk to an adult before meeting any online contacts.

Private

- I will keep my passwords private.
- I know I must always check my privacy settings are safe and private.
- I will think before sharing personal information ***and/or*** seek advice from an adult.

- I will keep my password safe and private as my privacy, Birchwood work and safety must be protected.

Responsible

- I will not access or change other people files, accounts, or information.
- I will only upload appropriate pictures or videos of others online and when I have permission.
- I know I must respect Birchwood systems and equipment and if I cannot be responsible then I will lose the right to use them.
- I will write emails and online messages carefully and politely as I know they could be forwarded or seen by someone I did not intend.
- I will only change the settings on the computer if a teacher has allowed me to.
- I know that use of the Birchwood ICT system for personal financial gain, gambling, political purposes, or advertising is not allowed.
- I understand that the Birchwood internet filter is there to protect me, and I will not try to bypass it.
- I know that if Birchwood suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices.
- I know that if I do not follow the Birchwood AUP then:
    - **I could lose my access to the School computer/laptop**
    - **My Parents/Carers will be informed**
    - **I could be excluded from Birchwood**
    - **I may be reported to the Police of online safety organisations for misuse.**

Kind

- I know that bullying in any form (on and offline) is not tolerated and I know that technology should not be used for harassment.
- I will not upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the Birchwood community.
- I will always think before I post as text, photos or videos can become public and impossible to delete.
- I will not use technology to be unkind to people.

Legal

- I know it can be a criminal offence to hack accounts or systems or send threatening and offensive messages.
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources.
- I understand that it may be a criminal offence or breach of the Birchwood policy to download or share inappropriate pictures, videos, or other material online.

Reliable

- I will always check that any information I use online is reliable and accurate.
- I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place, with a trusted adult present.

Report

- If I am aware of anyone trying to misuse technology, I will report it to a member of staff.
- I will speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared, or uncomfortable.
- I will visit www.thinkuknow.co.uk, www.childnet.com and www.childline.org.uk to find out more about keeping safe online.
- I have read and talked about these expectations with my parents/carers.

Learners with Special Educational Needs and Disabilities (SEND)

Learners with SEND functioning at Levels P4 –P7

- I ask a grown up if I want to use the computer
- I make good choices on the computer
- I use kind words on the internet
- If I see anything that I do not like online, I tell a grown up
- I know that if I do not follow the Birchwood rules then:
    - **I could lose my access to the School computer/laptop**
    - **My Parents/Carers will be informed**
    - **I could be excluded from Birchwood**
    - **I may be reported to the Police of online safety organisations for misuse.**

Learners with SEND functioning at Levels P7-L1

(Based on Childnet's SMART Rules: www.childnet.com)

Safe

- I ask a grown up if I want to use the computer
- I do not tell strangers my name on the internet
- I know that if I do not follow the Birchwood rules then:
    - **I could lose my access to the School computer/laptop**
    - **My Parents/Carers will be informed**
    - **I could be excluded from Birchwood**
    - **I may be reported to the Police of online safety organisations for misuse.**

Meeting

- I tell a grown up if I want to talk on the internet

Accepting

- I do not open messages or emails from strangers

Reliable

- I make good choices on the computer

Tell

- I use kind words on the internet
- If I see anything that I do not like online, I will tell a grown up

Learners with SEND functioning at Levels L2-4

(Based on Childnet's SMART Rules: www.childnet.com)

Safe

- I ask an adult if I want to use the internet
- I keep my information private on the internet
- I am careful if I share photos online
- I know that if I do not follow the Birchwood rules then:
  - **I could lose my access to the School computer/laptop**
  - **My Parents/Carers will be informed**
  - **I could be excluded from Birchwood**
  - **I may be reported to the Police of online safety organisations for misuse.**

Meeting

- I tell an adult if I want to talk to people on the internet
- If I meet someone online, I talk to an adult

Accepting

- I do not open messages from strangers
- I check web links to make sure they are safe

Reliable

- I make good choices on the internet
- I check the information I see online

Tell

- I use kind words on the internet
- If someone is mean online, then I will not reply. I will save the message and show an adult
- If I see anything online that I do not like, I will tell a teacher

Learner Acceptable Use Policy Agreement Form (if age appropriate)

Settings should attach a copy of an age appropriate AUP to this form. Settings may need to provide learners and parents with updated versions of the AUP as learners progress through the setting.

Birchwood Acceptable Use of Technology Policy – Learner Agreement

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

I agree to follow the AUP when:

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

Name…….. Signed……

Date……

Parent/Carers Name…….. (***If appropriate***)

Parent/Carers Signature…….. (***If appropriate***)

Date…….

Acceptable Use of Technology Statements and Forms for Parents/Carers

Parent/Carer AUP Acknowledgement

Birchwood- Learner Acceptable Use of Technology Policy Acknowledgment

1. I, with my child, have read and discussed Birchwood 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 Birchwood 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 Birchwood 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 Birchwood mobile technology policy states that my child cannot use personal device and mobile technology on site.

5. I understand that my child needs a safe and appropriate place to access remote learning if Birchwood is closed in response to Covid-19. I will ensure my child's access to remote learning is appropriately supervised. When accessing video learning, I will ensure they are an appropriate location (e.g. not in bed) and that they are suitably dressed.

6. I understand that Birchwood will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that the Birchwood cannot ultimately be held responsible for the nature and content of materials accessed on the internet or if my child is using mobile technologies.

7. I with my child, am 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 school community.

8. I understand that Birchwood will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety.

9. I will inform the Birchwood or other relevant organisations if I have concerns over my child's or other members of the school communities' safety online.

10. 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 school.

11. I will support Birchwood's 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.

Child's Name…….. Child's Signature …….... (***if appropriate***)

Class…… Date…….

Parents Name…….....

Parents Signature……... Date…….

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 Birchwood.

2. I am aware that learners use of mobile technology and devices, such as mobile phones, is not permitted at Birchwood.

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

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

5. I understand that my child needs a safe and appropriate place to access remote learning if Birchwood is closed in response to Covid-19. I will ensure my child's access to remote learning is appropriately supervised. When accessing video learning, I will ensure they are an appropriate location (e.g. not in bed) and that they are suitably dressed.

6. I am aware that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.

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

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

9. I know I can seek support from the school about online safety, such as via the school website (www.birchwoodpru.kent.sch.uk), to help keep my child safe online at home.

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

11. 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 school community.

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

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

14. I know that I can speak to the Designated Safeguarding Lead, Jane Waters or, my child's Teacher or the Head Teacher if I have any concerns about online safety.

I have read, understood and agree to comply with the Birchwood Parent/Carer Acceptable Use of Technology Policy.

Child's Name……..

Parent/Carers Name……..

Parent/Carers Signature……

Date…….

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 Birchwood 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 Birchwood expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that Birchwood 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 Birchwood 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 Birchwood Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school staff code of conduct and remote learning AUP.

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

Use of Birchwood Devices and Systems

4. I will only use the equipment and internet services provided to me by Birchwood for example school 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 educational use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed.

6. Where I deliver or support remote learning, I will comply with the Birchwood remote learning AUP.

Data and System Security

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
    - I will use a 'strong' password to access school systems.
    - I will protect the devices in my care from unapproved access or theft.

8. I will respect school system security and will not disclose my password or security information to others.

9. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the Business and Inclusion Manager or Head Teacher.

10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the Business and Inclusion Manager.

11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school information security policies.
    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school.

12. I will not keep documents which contain school related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school learning platform to upload any work documents and files in a password protected environment.

13. I will not store any personal information on the school IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.

14. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

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

16. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the Business and Inclusion Manager, Head Teacher or Cantium (EIS) as soon as possible.

17. If I have lost any school related documents or files, I will report this to the Business and Inclusion Manager, Head Teacher) and school Data Protection Officer (GDPRiS) as soon as possible.

18. Any images or videos of learners will only be used as stated in the school camera and 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

19. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in e.g. child protection, online safety, remote learning AUP.
20. I have read and understood the school mobile technology and social media policies
21. 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's (DSL) Jane Waters and Lee Palmer 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.

22. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the school child protection policies.

23. 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

24. I have read and understood the school policy which covers expectations regarding staff use of mobile technology and social media.
25. 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 code of conduct, 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 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 mobile technology 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 school staff code of conduct and the law.

26. 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 my line manager and Jane Waters and Lee Palmer Designated Safeguarding Leads (DSL).
- Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSLs.

27. 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's

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 is 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 school into disrepute.

Policy Compliance

31. I understand that the school 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

32. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the school child protection policy.

33. I will report concerns about the welfare, safety, or behaviour of staff to the Head Teacher in line with the allegations against staff policy.

34. 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 staff code of conduct.

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

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

I have read, understood and agreed to comply with Birchwood 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 ……..

Visitor and Volunteer Acceptable Use of Technology Policy

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 Birchwood ensure that all visitors and volunteers understand the school 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 Birchwood 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 Birchwood AUP should be read and followed in line with the school 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 school ethos, school 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.

Classroom Practice

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

6. Where I deliver or support remote learning, I will comply with the school/setting remote learning AUP.

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's) Jane Waters, Lee Palmer in line with the school 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 Social Media and Mobile Technology

10. I have read and understood the school 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/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 school staff code of conduct policy 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's, Jane Waters or Lee Palmer.

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(s), Jane Waters or Lee Palmer.

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 school 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's (Jane Waters or Lee Palmer) in line with the school child protection policy.

19. I will report concerns about the welfare, safety, or behaviour of staff to the head teacher, 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.

I have read, understood and agreed to comply with Birchwood PRU 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 ……..

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list and all members of the school community are reminded that technology use should be consistent with our ethos, other appropriate policies, and the law.

1. The school provides Wi-Fi for the school community and allows access for education use

2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the school premises that is not the property of the school.

3. The use of technology falls under Birchwood PRU, Acceptable Use of Technology Policy (AUP), online safety policy and staff code of conduct policy (***any other relevant policies such as data protection, safeguarding/child protection***) which all learners/staff/visitors and volunteers must agree to and comply with.

4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. School owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

6. I will take all practical steps necessary to make sure that any equipment connected to the school service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The school wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

10. I will not attempt to bypass any of the school security and filtering systems or download any unauthorised software or applications.

11. My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead's (Jane Waters and Lee Palmer) as soon as possible.

14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead's (Jane Waters and Lee Palmer)

15. I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agreed to comply with Birchwood Wi-Fi acceptable Use Policy.

Name ……...

Signed: ……..Date……

Template Acceptable Use Policy (AUP) for Remote Learning and Online Communication

These templates specifically address safer practice when running formal remote learning, including live streamed sessions, but can also apply to other online communication, such as remote parent meetings or pastoral activities. There is no expectation that staff should run formal live streamed sessions or provide pre-recorded videos; settings should implement the approaches that best suit the needs of their community and staff following appropriate discussions.

This content can either be used to create a standalone AUP or can be integrated into existing documents according to setting preference.

A remote learning AUP should be completed following a thorough evaluation of remote learning tools with approval from leadership staff. We recommend settings use existing systems and/or education focused platforms where possible, and that staff only use approved accounts and services to communicate with learners and/or parents/carers.

Additional information and guides on specific platforms can be found at:

- https://coronavirus.lgfl.net/safeguarding
- https://swgfl.org.uk/resources/safe-remote-learning/video-conferencing-for-kids-safeguarding-and-privacy-overview/

Further information and guidance for SLT and DSLs regarding remote learning:

- Local guidance:
  - Kelsi: Guidance for Full Opening in September
    - Online Safety Guidance for the Full Opening of Schools
  - The Education People:' 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 Template - Staff Statements

Birchwood PRU - Staff Remote Learning AUP

The Remote Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of school 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 Doddle and Zoom.
    - These systems have been assessed and approved by the head teacher.
2. Staff will only use school 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 Jane Waters or Lee Palmer, Designated Safeguarding Leads (DSL).
    - Staff will use work provided equipment where possible e.g. a school laptop.
3. Online contact with learners and/or parents/carers will not take place outside of the operating times as defined by the Head Teacher.
4. All remote lessons will be formally timetabled; a member of SLT, DSL and/or head of department is able to drop in at any time.
5. Live streamed remote learning sessions will only be held with approval and agreement from the head teacher.

Data Protection and Security

6. All remote learning and any other online communication will take place in line with current school confidentiality expectations as outlined in data protection policy.
7. Staff will not record lessons or meetings using personal equipment.
8. Only members of Birchwood community will be given access to Doodle or Zoom.
9. Access to these systems will be managed in line with current IT security expectations as outlined in AUP and Data protection policy.

Session Management

Staff will record the attendance of any sessions held.

Appropriate privacy and safety settings will be used to manage access and interactions. This includes:

- Disabling chat, staff not permitting learners to share screens, keeping meeting IDs private, use of waiting rooms/lobbies or equivalent.

10. 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.

11. 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.
    - 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.
12. Alternative approaches and/or access will be provided to those who do not have access.

Behaviour Expectations

13. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
14. All participants are expected to behave in line with existing school policies and expectations. This includes:
    - Appropriate language will be used by all attendees.
    - Staff will not take or record images for their own personal use.
    - 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.
15. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
16. 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.
17. 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

18. Participants are encouraged to report concerns during remote and/or live streamed sessions:
19. 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 Jane Waters, Head Teacher or Lee Palmer, Business and Inclusion Manager.
20. 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.
21. Sanctions for deliberate misuse may include: restricting/removing use, contacting police if a criminal offence has been committed.
22. Any safeguarding concerns will be reported to Jane Waters or Lee Palmer, Designated Safeguarding Leads, in line with our child protection policy.

I have read and understood the Birchwood PRU Acceptable Use Policy (AUP) for remote learning.

Staff Member Name: ……

Date……

Birchwood PRU - Learner Remote Learning AUP

I understand that:

- these expectations are in place to help keep me safe when I am learning at home using Doddle or Zoom or other learning platform.
- I should read and talk about these rules with my parents/carers.
- remote learning will only take place using the named learning platform and during usual school times.
- My use of the identified learning platform is monitored to help keep me safe.

2. Only members of Birchwood community can access Doddle or Zoom or other learning platform.
   - I will only use my school provided email accounts and/or login to access remote learning.
   - I will use privacy settings as agreed with my teacher/set up the school/setting.
   - I will not share my login/password with others
   - I will not share any access links to remote learning sessions with others.

3. When taking part in remote learning I will behave as I would in the classroom. This includes:
   - Using appropriate language.
   - Not taking or recording images/content without agreement from the teacher and/or those featured.

4. When taking part in live sessions I will:
   - Mute my video and microphone.
   - wear appropriate clothing and be in a suitable location.
   - Attend the session in full. If for any reason I cannot attend a session in full, I will let my teacher know.
   - attend lessons in a shared/communal space or room with an open door and/or where possible when I can be supervised by a parent/carer or another appropriate adult.

5. If I am concerned about anything that takes place during remote learning, I will:
   - Report concerns to the member of staff running the session, tell a parent/carer etc.

6. I understand that inappropriate online behaviour or concerns about my safety during remote learning will be taken seriously. This could include:
   - restricting/removing access, informing parents/carers, contacting police if a criminal offence has been committed.

I have read and understood the Birchwood Acceptable Use Policy (AUP) for remote learning.

Name…….. Signed…….

Class…… Date…….

Parent/Carers Name…….. (***If appropriate***)

Parent/Carers Signature…….. (***If appropriate***)