Policy Title	**Acceptable Use of Technology Policy**

Policy Reference	**Education People Model template Sept 2022**
Function	For Information and Guidance
Status	Statutory
Audience	Parents, Governors, Headteacher, Teachers, Support Staff, the Department for Education
Ownership / Implementation	The Headteacher and the Governing Body have overall responsibility for ensuring that this policy is implemented.
Staff member responsible	Headteacher
Review Frequency	Annual
Approved by Staff & Pupil Welfare Committee	Approved 23rd May 2023
Date Approved by Governing Body	Responsibility delegated to the Staff and Pupil Welfare committee
Date for Review	May 2024

Acceptable Use of Technology Policy Templates for Educational Settings

September 2022

Contents

THE EDUCATION PEOPLE

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.

- **Blue font** indicates that the setting should insert relevant information
- **Pink font** highlights suggestions to assist DSLs, leaders and managers in amending sample statements and ensuring content is appropriate for their setting. This content is provided as guidance notes and should not be left in individual settings policies

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.
  - o 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 response 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.

THE EDUCATION PEOPLE

Updated content for 2021

The core content within the AUP template for 2021 has been updated and remains much the same as 2020.

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.

The copyright of these materials is held by The Education People. However, educational settings that work with children and young people are granted permission to use all or part of the materials for not for profit use, providing the Education People copyright is acknowledged and we are informed of its use.

THE EDUCATION
PEOPLE

Learner Acceptable Use of Technology Statements

Key Stage 2 (7-11)

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

- I understand that the Amherst School internet filter is there to protect me, and I will not try to bypass it.
- I know that all Amherst School 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.

- I understand that the Amherst School Acceptable Use Policy will help keep me safe and happy online at home and at school.
- I know that I will be able to use the internet in Amherst School for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at Amherst School
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these I should report it to a teacher or adult in Amherst School, or a parent or carer at home.
- I will treat my password like my toothbrush! This means I will not share it with anyone (even my best friend), and I will log off when I have finished using the computer or device.
- I will protect myself by not telling anyone I meet online my address, my telephone number, my Amherst School name or by sending a picture of myself without permission from a teacher or other adult.
- I will not arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- If I get unpleasant, rude, or bullying emails or messages, I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.
- I will always check before I download software or data from the internet. I know that information on the internet may not be reliable and it sometimes needs checking.
- If I bring in memory sticks / CDs from outside of Amherst School I will always give them to my teacher so they can be checked for viruses and content before opening them.
- I will be polite and sensible when I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.
- I know that I am not allowed on personal email, social networking sites or instant messaging in Amherst School.

6

THE EDUCATION PEOPLE

- If, for any reason, I need to bring my mobile phone into Amherst School I know that it is to be handed in to the office and then collected at the end of the school day.
- I know that all Amherst School devices/computers and systems are monitored, including when I am using them at home.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.

THE EDUCATION PEOPLE

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

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

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

Meeting

- I tell an adult if I want to talk to people on the internet

THE EDUCATION PEOPLE

- 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.

THE EDUCATION
PEOPLE

Acceptable Use of Technology Sample Statements and Forms for Parents/Carers

Parent/Carer AUP Acknowledgement

Amherst School

Learner Acceptable Use of Technology Policy Acknowledgment

1. I, with my child, have read and discussed Amherst School learner acceptable use of technology policy (AUP) and understand that the AUP will help keep my child safe online.

2. I understand that the AUP applies to my child use of Amherst School 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 Amherst School 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 Amherst School mobile technology policy states that my child cannot use personal device and mobile technology on site. All mobile phones must be handed in to the office on arrival and collected at the end of the school day.

5. I understand that my child needs a safe and appropriate place to access remote learning if Amherst School 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 the school 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 school 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 the school 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 school 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.

THE EDUCATION PEOPLE

11. I will support the school 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 …………………………………...

Class……………………………… Date……………………….

Parents Name……………………………………………….............................

Parents Signature………………………………………………………………... Date…………….

THE EDUCATION
PEOPLE

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 IT suite desktop computers, laptops and iPads in order to access the curriculum and be prepared for modern life whilst at Amherst School.

2. I am aware that learners use of mobile technology and devices, such as mobile phones, is not permitted at Amherst School. If a child brings a mobile phone to school it must be handed in to the office on arrival and collected at the end of the day.

3. I am aware that any internet and technology use using school 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 the school 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 the school 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 school 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 Amherst School learner Acceptable Use of Technology Policy (AUP) with my child.

8. I will support school 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.amherst.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 Amherst School 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 (headteacher, assistant headteacher and SENCO), or my child's teacher if I have any concerns about online safety.

THE EDUCATION PEOPLE

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

Child's Name…………………………………………… Class…………………………

Parent/Carers Name………………………………………...

Parent/Carers Signature…………………….……………………………………………..

Date…………………….

THE EDUCATION PEOPLE

Acceptable Use of Technology for Staff, Visitors and Volunteers Sample Statements

Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Amherst School IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for learners, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand Amherst School expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy Scope

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

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

Use of Amherst School Devices and Systems

3. I will only use the equipment and internet services provided to me by the school for example school provided laptops, tablets, mobile phones, and internet access, when working with learners.

4. 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.

Data and System Security

5. 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.

THE EDUCATION PEOPLE

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

7. 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 headteacher or school business manager.

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

9. 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.
    o   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.
    o   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.

10. 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.

11. 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.

12. 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.

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

14. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the headteacher or school business manager as soon as possible.

15. If I have lost any school related documents or files, I will report this to the headteacher or school business manager and school Data Protection Officer (SATSWANA) as soon as possible.

16.

THE EDUCATION PEOPLE

o 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

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

18. 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:
   o exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
   o 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.
   o involving the Designated Safeguarding Lead (DSL) (Andrew Reid) or a deputy (Trish Jones and Lyndsey Billing) 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.
   o make informed decisions to ensure any online safety resources used with learners is appropriate.

19. 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.

20. 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

Expectations
- The expectations' regarding safe and responsible use of social media applies to all members of Amherst School community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Amherst School community are expected to engage in social media in a positive, safe and responsible manner.
   o All members of Amherst School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site.

THE EDUCATION PEOPLE

- o The use of social media during teaching hours for personal use **is not** permitted.
- o Inappropriate or excessive use of social media during teaching hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of Amherst School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

Staff Personal Use of Social Media
- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy.

Reputation
- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
  - o Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
  - o Setting the privacy levels of their personal sites.
  - o Being aware of location sharing services.
  - o Opting out of public listings on social networking sites.
  - o Logging out of accounts after use.
  - o Keeping passwords safe and confidential.
  - o Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of Amherst School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

THE EDUCATION PEOPLE

Communicating with learners and their families

• Staff will not use any personal social media accounts to contact learners or their family members.
• All members of staff are advised not to communicate with or add any current or past learners or their family members, as 'friends' on any personal social media accounts.
• Any communication from learners and parents/carers received on personal social media accounts will be reported to the DSL (or deputy) and/or the headteacher/manager. Amend as appropriate.
• Any pre-existing relationships or situations, which mean staff cannot comply with this requirement, will be discussed with the Headteacher. Decisions made and advice provided in these situations will be formally recorded to safeguard learners, members of staff and the setting.
• If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.

21. 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 and the headteacher.

22. 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.

23. 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.

24. 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.

Use of Personal Devices and Mobile Phones

● Amherst School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

Expectations

● All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.
● Electronic devices of any kind that are brought onto site are the responsibility of the user.

THE EDUCATION PEOPLE

- o All members of Amherst School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- o All members of Amherst School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of Amherst School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: AUP and Staff Handbook.
- Staff will be advised to:
    - o Keep mobile phones and personal devices in a safe and secure place during lesson time.
    - o Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
    - o Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
    - o Not use personal devices during teaching periods, unless written permission has been given by the Headteacher, such as in emergency circumstances.
    - o Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
    - o Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy) or Headteacher.
- Staff will not use personal devices:
    - o To take photos or videos of learners and will only use work-provided equipment for this purpose.
    - o Directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy

THE EDUCATION PEOPLE

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

Visitors' Use of Personal Devices and Mobile Phones

- Parents/carers and visitors (including volunteers and contractors) should ensure that phones are used in accordance with this policy.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Visitors (including volunteers and contractors) who are on site for a regular or extended period will use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or Headteacher of any breaches our policy.

Policy Compliance

25. 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

26. 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.

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

28. 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 School Discipline and Conduct Policy.

29. 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/setting may invoke its disciplinary procedures as outlined in the School Discipline and Conduct Policy.

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

THE EDUCATION PEOPLE

I have read, understood and agreed to comply with Amherst School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member: ……………………………………………………………………………

Signed: ……………………………………………………………………………………………....

Date (DDMMYY)…………………………………………………...

THE EDUCATION PEOPLE

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

THE EDUCATION PEOPLE

Remote Learning AUP Template - Staff Statements

Amherst School

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 Google Classroom and Zoom for live sessions.

2. Staff will only use school managed **or** specific, approved professional accounts with learners **and** parents/carers.
   - Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
     - o Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with Andrew Reid, Designated Safeguarding Lead (DSL).
   - Staff will use work provided equipment where possible
3. Online contact with learners and parents/carers will not take place outside of the operating times of the normal school day which is 8.30am – 5.30pm.
4. All remote lessons will be formally timetabled
5. Live streamed remote learning sessions will only be held with approval and agreement from the headteacher.

Data Protection and Security

6. Any personal data used by staff and captured by Google Classroom when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
7. All remote learning and any other online communication will take place in line with current school confidentiality expectations.
8. Only members of school community will be given access to Google Classroom.
9. Access to Google Classroom will be managed in line with current IT security expectations.

Session Management

10. When live streaming with learner
    - contact will be made via learners' school provided Google Classroom account.
    - staff will mute learners' microphones.

11. Live 1 to 1 sessions will only take place with approval from the headteacher.
12. A pre-agreed invitation via Google Classroom 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 appropriately supervised by a parent/carer or another

THE EDUCATION PEOPLE

appropriate adult. A second adult should be present in addition to the member of staff.

13. Alternative approaches access will be provided to those who do not have access.

Behaviour Expectations

14. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
15. 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.
16. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
17. 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.
18. 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

19. Participants are encouraged to report concerns during remote and live streamed sessions.
20. 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 headteacher.
21. 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.
22. Sanctions for deliberate misuse may include restricting/removing use, contacting police if a criminal offence has been committed.
23. Any safeguarding concerns will be reported to Andrew Reid, Designated Safeguarding Lead, in line with our child protection policy.

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

Staff Member Name: ………………………………………………………………….

Date…………………………

THE EDUCATION PEOPLE

Remote Learning AUP Template - Learner Statements

Amherst School

Learner Remote Learning AUP

I understand that:

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

2. Only members of Amherst School community can access Google Classroom.
   - I will only use my school provided login to access remote learning.
   - I will use privacy settings as agreed with my school.
   - 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 microphone.
   - wear appropriate clothing and be in a suitable location.
   - ensure backgrounds of videos are neutral and personal information/content is not visible.
   - Use appropriate alternative backgrounds.
   - 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 let my teacher know.
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 Amherst School Acceptable Use Policy (AUP) for remote learning.

Name……………………………………………… Signed……………………….

Class……………………… Date……………………

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

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

Acknowledgements and thanks

These statements have been produced by The Education People Education Safeguarding Service.

Theeducationpeople.org

THE EDUCATION PEOPLE