Amherst School (Academy) Trust

Acceptable Use of Technology Policy

Policy Title	**Acceptable Use of Technology Policy**

Policy Reference	**Education People Model template - August 2025**
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	23 April 2026
Date Approved by Governing Body	Responsibility delegated to the Staff and Pupil Welfare committee
Date for Review	May 2027

Acceptable Use of Technology Policy Templates for Educational Settings 2025-26

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) 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 children/pupils/students and technology available.

Key Points

- AUPs should be recognised by educational settings as part of the portfolio of safeguarding policies and as part of the code of conduct and/or behaviour policies.
- AUPs are not technical policies and as such oversight and development will fall within the role and responsibilities of the Designated Safeguarding Lead (DSL) and overall approval from SLT, including governing boards/trusts etc.
    - 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 IT providers/staff, therefore leaders should ensure that time is allocated to ensure this takes place.
- Where possible and appropriate, children/pupils/students, 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 changes to technology use made.
- Leaders should consider how they evidence that all members of the community have read and understood these policies, for example, keeping copies of signed agreements, publishing AUPs on the school/setting website and intranet.
- AUPs can be used to support other policies and training and education approaches to ensure there is a clear understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring.
- 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 or provide children/pupils/students and/or staff with individual devices.

Using this document

- **Blue font** indicates that the setting should amend and/or insert relevant information.
- **Red 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.

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. Academy trusts, federations or chains of settings may wish to use these templates across their entire organisation, however AUPs will need to be adapted to suit the needs of each individual provision.

It will not be appropriate for educational settings to adopt the templates in their entirety; DSLs and leaders should ensure that any unnecessary content is removed.

Filtering and Monitoring

Schools and settings should ensure their AUPs reflect their specific approaches and the systems in place in relation to appropriate filtering and monitoring. We recommend DSLs and leaders access the following national guidance to support the decision making.

- Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - DfE Guidance
- Appropriate Filtering and Monitoring Guidance - UK Safer Internet Centre
- Filtering and monitoring - Questions for governors, proprietors and trustees - UK Safer Internet Centre
- Filtering and Monitoring Webinars - SWGfL

Use of Artificial Intelligence

Kent County Council recognises that generative artificial intelligence (AI) tools may have many uses which could benefit education settings community. However, it is important to recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material, and additionally its use can pose moral, ethical and legal concerns.

This template does not fully reflect the use of AI as individual education leaders will need to make informed decisions regarding whether and how AI is used/permitted within their community. Where settings do permit use, we recommend these templates are adapted to reflect your specific expectations for use by staff and pupils/students as appropriate.

Leaders may need/wish to refer to use of AI in their child protection policy and other relevant curriculum-based policies according to leadership decisions in relation to the use (or not) of AI tools. The following links may also provide further information for leaders to consider:

- Generative artificial intelligence (AI) in education - GOV.UK (www.gov.uk)
- Data protection in schools - Artificial intelligence (AI) and data protection in schools - Guidance - GOV.UK (www.gov.uk)
- Artificial Intelligence and Online Safety | SWGfL
- Using artificial intelligence (AI) safely | Internet Matters

Disclaimer

Kent County Council 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 Kent County Council. 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 Kent County Council copyright is acknowledged and we are informed of its use.

Child/Pupil/Student Acceptable Use of Technology Statements

Key Stage 2 (7-11)

- I understand that the 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 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 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 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 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 School.
- I know that I am not allowed to bring a smartphone or smart device such as a smartwatch to Amherst School. A smart device is a device that can connect to the internet.
- I understand that I must not bring a watch/device to school that contains a camera.
- I understand that if I bring a mobile phone (that is not a smartphone) to Amherst School it must 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.
- I will not use technology to be unkind to people.
- I will keep information about me and my passwords private.
- I always talk to an adult if I see something which makes me feel worried.
- I know my use of Amherst School devices and systems can be monitored.
- I will only change the settings on the computer if a teacher has allowed me to.
- I know that use of the Amherst School ICT system for personal financial gain, gambling, political purposes, or advertising is not allowed.
- I understand that the Amherst School internet filter is there to protect me, and I will not try to bypass it.
- I know that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring approaches may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices.
- 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 know I must respect the Amherst School systems and equipment and if I cannot be responsible then I will lose the right to use them.
- I have read and talked about these rules with my parents/carers.
- I know that if I do not follow the Amherst School AUP then the Behaviour Policy will be followed.

Children/Pupils/Students 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 Amherst School rules then the Behaviour Policy will be followed.

Learners with SEND functioning at Levels P7-L1 (Based on Childnet's SMART Rules)

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 Amherst School rules then the Behaviour Policy will be followed.

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)

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 Amherst School rules then the Behaviour Policy will be followed.

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.

Acceptable Use of Technology Statements and Forms for Parents/Carers

Parent/Carer AUP Acknowledgement Form

Amherst School Pupil Acceptable Use of Technology Policy Acknowledgment

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

2. I understand that the AUP applies to my child's use of Amherst School devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another pupil, could have repercussions for the orderly running of the school, if a pupil is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.

3. I understand that any use of Amherst School devices and systems are appropriately filtered. Amherst School Web Filtering & Online Protection is provided by Netsweeper through our Internet provider (MGFL). The service provides safe, filtered, and logged web access for both staff and pupils through the school's broadband connection. It also provides a monitoring and alerting service that helps safeguard pupils.

4. I am aware that my child's use of Amherst School provided devices and systems will be monitored for safety and security reasons, when used on and offsite. Monitoring approaches are in place 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.

5. I understand that Amherst School will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use school devices and systems, on and offsite. I however understand that Amherst School cannot ultimately be held responsible for filtering breaches that occur due to the dynamic nature of materials accessed online, or if my child is using a personal device, including mobile or smart technologies.

6. I understand that my child is not allowed to bring a smartphone or smart device such as a smartwatch to Amherst School. A smart device is a device that can connect to the internet.

7. I understand that I must not bring a watch/device to school that contains a camera.

8. I understand that if I bring a mobile phone (that is not a smartphone) to Amherst School it must be handed in to the office and then collected at the end of the school day.

9. I understand that my child needs a safe and appropriate place to access remote/online learning, for example, if the school is closed. I will ensure my child's access to remote/online learning is appropriately supervised and any use is in accordance with the school remote learning AUP.

10. I and my child are aware of the importance of safe online behaviour and will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the school community, or content that could adversely affect the reputation of Amherst School.

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

12. I will inform the school (for example speaking to a member of staff and/or the Designated Safeguarding Lead) or other relevant organisations if I have concerns over my child's or other members of the school community's safety online.

13. 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 Amherst School.

14. I understand my role and responsibility in supporting Amherst School's online safety approaches and safeguarding my child online. I will use parental controls, supervise access 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……

Parent/Carer's Name…….....

Parent/Carer's Signature……...

Date…….

Acceptable Use of Technology for Staff, Visitors and Volunteers

Staff Acceptable Use of Technology Policy (AUP)

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 pupils, 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's 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 Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school or accessed by me as part of my role within Amherst School, professionally and personally, both on and offsite. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email. data and data storage, remote learning systems and communication technologies**.**

2. I understand that Amherst School's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school child protection policy, staff code of conduct and handbook.

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 school devices and systems

4. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed; this use at the school's discretion and can be revoked at any time.

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

Data and system security

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

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

8. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager (Andy Holden – Cantium), school business manager or headteacher.

9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager (Andy Holden – Cantium), school business manager or headteacher.

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

11. 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 or school provided VPN.

12. 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.

13. 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.

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

15. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the the IT system manager (Andy Holden – Cantium), school business manager or headteacher as soon as possible.

16. If I have lost any school related documents or files, I will report this to the IT system manager, school business manager or headteacher and school Data Protection Officer (Karen Wicks School Business Manager) as soon as possible.

17. Any images or videos of pupils will only be used as stated in the school camera and image use policy. I understand images of pupils must always be appropriate and should only be taken with school provided equipment and only be taken/published where pupils and/or parent/carers have given explicit written consent.

Classroom practice

18. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by Amherst School as detailed in child protection policy and staff code of conduct and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.

19. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and headteacher, in line with the school child protection policy and staff code of conduct.

20. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in child protection policy, remote learning AUP and staff code of conduct.

21. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I also recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material. Additionally, its use can pose moral, ethical and legal concerns if not carefully managed.

    As such, I understand that the use of AI as part of our education/curriculum approaches is permitted by staff but not pupils:
    - Use of AI to support curriculum planning/creating resources will be shared with the school leadership team to monitor the appropriateness of its use.
    - Use of AI by the admin team should be shared with the School Business Manager and Headteacher to monitor the appropriateness of its use.
    - AI should not be used to write pupils' individual school reports.

- I am required to critically evaluate any AI-generated content for accuracy, bias, and appropriateness before sharing or using it in educational contexts.
- AI must not be used to replace professional judgement, especially in safeguarding, assessment, or decision-making involving children.
- Any misuse of AI will be responded to in line with relevant school policies, including but not limited to, anti-bullying, staff and pupil behaviour and child protection.

22. I will promote online safety with the pupils 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 pupil feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) (Andrew Reid) or deputies (Trish Jones and Becky Watson) as part of planning online safety lessons or activities to ensure support is in place for any pupils who may be impacted by the content.
    - Informing the DSL and/or leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
    - make informed decisions to ensure any online safety resources used with pupils is appropriate.

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.

Mobile devices and smart technology

24. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff code of conduct and the school mobile technology policy and the law. I understand that I am not permitted to make / receive personal calls / texts, send / receive emails or access internet / social media during work time where children are present.

    I will ensure that mobile devices are silent at all times whilst in the classroom or where children are present. Mobile devices should not be left on display.

    I will not use my personal equipment (mobile phones / cameras / tablets) to take photos or make recordings of pupils / students *unless given explicit instruction to do so by the headteacher or chair of governors in respect of the headteacher*

Online communication, including use of social media

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

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

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

Policy concerns

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

29. I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

30. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of Amherst School into disrepute.

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

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

Policy Compliance and Breaches

33. If I have any queries or questions regarding safe and professional practise online, either in school or off site, I will raise them with the DSL and the headteacher.

34. I understand that the school may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of pupils and staff. This includes monitoring all school provided devices and school systems and networks including school provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

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

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

37. 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 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)……..

Template Acceptable Use Policy (AUP) for Remote/Online Learning

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

- LGfL: Safeguarding Considerations for Remote Learning
- SWGfL: Which Video Conference platform is best?

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

- Local guidance:
  - Kelsi:
    - Online Safety Guidance for the Full Opening of Schools
  - The Education People: Covid-19 Specific Safeguarding Guidance and Resources
    - 'Safer remote learning during Covid-19: Information for School Leaders and DSLs'
- National guidance:
  - DfE: 'Safeguarding and remote education during coronavirus (COVID-19)
  - SWGfL: Safer Remote Learning
  - NSPCC: Undertaking remote teaching safely
  - Safer Recruitment Consortium: Guidance for safer working practice

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.
     - 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.
    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 appropriate adult. A second adult should be present in addition to the member of staff.
12. Alternative approaches 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 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 the headteacher.
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 Andrew Reid, Designated Safeguarding Lead, in line with our child protection policy.
23.

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

Staff Member Name: ……

Date…….

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…….....

Parent/Carers Signature…….

Acknowledgements and Thanks

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

Additional thanks to members of the Kent Education Online Safety Strategy Group, the UK Safer Internet Centre, South West Grid for Learning (SWGfL), London Grid for Learning (LGfL), South East Grid for Learning (SEGfL), Childnet, CEOP, The Judd School, Kingsnorth Primary School, Loose Primary School, Peter Banbury, Kent Police, Kent Schools Personnel Service (SPS), Kent Legal Services and Kent Libraries and Archives, for providing comments, feedback and support on previous versions.