# Acceptable Use of Technology Policy Templates for Educational Settings 2024-25

**Published August 2024**

# Contents

[Using the AUP Templates: Guidance Notes 3](#_Toc141779698)

[Child/Pupil/Student Acceptable Use of Technology Sample Statements 5](#_Toc141779699)

[Early Years and Key Stage 1 (0-6) 5](#_Toc141779700)

[Key Stage 2 (7-11) 6](#_Toc141779701)

[Key Stage 3/4/5 (11-18) 8](#_Toc141779702)

[Children/Pupils/Students with Special Educational Needs and Disabilities (SEND) 13](#_Toc141779703)

[Acceptable Use of Technology Sample Statements and Forms for Parents/Carers 16](#_Toc141779704)

[Parent/Carer AUP Acknowledgement Form 16](#_Toc141779705)

[Sample Parent/Carer Acceptable Use of Technology Policy (AUP) 18](#_Toc141779706)

[Acceptable Use of Technology for Staff, Visitors and Volunteers Sample Statements 20](#_Toc141779707)

[Staff Acceptable Use of Technology Policy (AUP) 20](#_Toc141779708)

[Visitor and Volunteer Acceptable Use of Technology Policy 26](#_Toc141779709)

[Wi-Fi Acceptable Use Policy 29](#_Toc141779710)

[Template Acceptable Use Policy (AUP) for Remote/Online Learning 31](#_Toc141779711)

[Remote/Online Learning AUP Template - Staff Statements 32](#_Toc141779712)

[Remote/Online Learning AUP Template – Pupil/Student Statements 36](#_Toc141779713)

[Acknowledgements and Thanks 39](#_Toc141779714)

# 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’](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2) (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](https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring)
* [Filtering and monitoring - Questions for governors, proprietors and trustees - UK Safer Internet Centre](https://saferinternet.org.uk/blog/filtering-and-monitoring-questions-for-governors-proprietors-and-trustees)
* [Filtering and Monitoring Webinars - SWGfL](https://swgfl.org.uk/resources/filtering-and-monitoring/)

**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)](https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education)
* [Data protection in schools - Artificial intelligence (AI) and data protection in schools - Guidance - GOV.UK (www.gov.uk)](https://www.gov.uk/guidance/data-protection-in-schools/artificial-intelligence-ai-and-data-protection-in-schools)
* [Artificial Intelligence and Online Safety | SWGfL](https://swgfl.org.uk/topics/artificial-intelligence/)
* [Using artificial intelligence (AI) safely | Internet Matters](https://www.internetmatters.org/tech-and-kids-digital-futures/using-artificial-intelligence-safely/)

**Updated content for 2024-25**

The core content within the AUP template for 2024-25 has been updated and remains much the same as 2024-25. Additional content or changes have been highlighted in yellow.

**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 Sample Statements

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

Settings should ensure their AUP includes age and ability appropriate information and expectations relating to the specific use and monitoring of school/setting provided devices and networks, services and/or systems, for example laptops, tablets and cloud computing, as well as use of learner owned devices such as mobile/smart phones, tablets and wearable technology.

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

### Early Years and Key Stage 1 (0-6)

* I understand that the school/setting Acceptable Use Policy will help keep me safe and happy online.
* I only use the internet when an adult is with me.
* I only click on online links and buttons when I know what they do. If I am not sure, I ask an adult first.
* I keep my personal information and passwords safe.
* I only send messages online which are polite and friendly.
* I know the school/setting can see what I am doing online when I use school/setting computers/tablets and name of any specific school/setting services and systems learners are expected to use, including if I use them at home. **Amend as appropriate to technology use by the age group, and to reflect your monitoring approaches.**
* I always tell an adult/teacher/member of staff if something online makes me feel upset, unhappy, or worried.
* I can visit [www.ceopeducation.co.uk](http://www.ceopeducation.co.uk) (**include other age-appropriate links**) to learn more about keeping safe online.
* I know that if I do not follow the school/setting rules:
	+ **List sanctions**
* I have read and talked about these rules with my parents/carers.

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

* I only go online with a grown-up.
* I am kind online.
* I keep information about me safe online.
* I tell a grown-up if something online makes me unhappy or worried.

### Key Stage 2 (7-11)

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

**Safe**

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

**Learning**

**Settings should include specific information and expectations relating to the use of devices and technology, for example, tablets, laptops, cloud computing, artificial intelligence (AI), shared file storage areas.**

* I ask my teacher before using my own personal smart devices and/or mobile phone at school/setting. **Other statements will be required if phones and personal devices are or are not permitted by the setting.**
* I always ask permission from an adult before using the internet.
* I only use websites and search engines that my teacher has chosen.
* I use school/setting devices for school/setting work unless I have permission otherwise.
* If I need to learn online at home, I will follow the school/setting remote/online learning AUP. **If school/setting does not have a separate remote learning AUP then appropriate content should be included here.**

**Trust**

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

**Responsible**

* I keep my personal information safe and private online.
* I will keep my passwords safe and will not share them.
* I will not access or change other people’s files or information.
* I will only change the settings on a device if a member of staff has allowed me to.

**Tell**

* If I see anything online that I should not or if I see something online that makes me feel worried or upset, I will…. **Amend to reflect your approach, for example, minimise the screen, shut the laptop lid, turn off the screen** and tell an adult immediately.
* If I am aware of anyone being unsafe with technology, I will report it to a teacher/adult at school/setting.
* I know it is not my fault if I see, or someone sends me, something upsetting or unkind online.
* I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.

**Understand**

* I understand that the school/setting internet filter is there to protect me, and I will not try to bypass it.
* I know that all school/setting owned devices and networks are monitored to help keep me safe, including if I use them at home. This means someone at the school/setting may be able to see and/or check my online activity when I use school/setting devices and/or networks if they are concerned about my or anyone else’s safety or behaviour. **Amend as appropriate to technology use by the age group, and to reflect your monitoring approaches.**
* If, for any reason, I need to bring a personal device, for example a smart/mobile phone and/or other wearable technology into school/setting then I will…. **Insert expectations as according to individual school/setting policy decisions, for example, I know that it is to be handed in to the office and then collected at the end of the school/setting day.**
* I have read and talked about these rules with my parents/carers.
* I can visit [www.ceopeducation.co.uk](http://www.ceopeducation.co.uk) and [www.childline.org.uk](http://www.childline.org.uk) to learn more about being safe online or to see help. **Add other websites or support services as appropriate.**
* I know that if I do not follow the school/setting rules then:
	+ **List sanctions**

**Alternative KS2 Statements**

(With thanks to Kingsnorth Primary School)

**Settings should amend and include specific information and expectations relating to their decisions relating to children’s use of devices and technology; for example, tablets, laptops, cloud computing, artificial intelligence (AI), shared file storage areas.**

* I understand that the school/setting 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/setting 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/setting.
* 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/setting, 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/setting 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 school/setting, 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/setting. **Other statements will be required access to personal email/social media is permitted by the setting.**
* If, for any reason, I need to bring a personal/smart device and/or mobile phone into school/setting I know that it is to be handed in to the office and then collected at the end of the school/setting day. **Amend as appropriate to the settings mobile/smart technology policy.**
* I know that all school/setting 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.

**Shortened KS2 version (for use on posters)**

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

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

* I understand that the school/setting Acceptable Use Policy will help keep me safe and happy online at home and at school.
* I know that school/setting 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. **Settings should include specific information and expectations relating to the use of devices and technology, for example, tablets, laptops, cloud computing, artificial intelligence (AI), shared file storage areas.** If I am not sure if something is allowed, I will ask a member of staff.
* I know that my use of school/setting devices and school/setting provided systems and internet access will be monitored to keep me safe and ensure policy compliance. **Amend as appropriate to technology use by the age group, and to reflect your monitoring approaches.**
* I will keep my password safe and private as my privacy, school/setting work and safety must be protected.
* If I need to learn online at home, I will follow the school/setting remote/online learning AUP. **If school/setting does not have a separate AUP then appropriate content should be included here.**
* 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. **Amend according to social media policy - remove this statement if access is not permitted at any time.**
* 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 at school/setting name, and technology should not be used for harassment of any type.
* 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 school/setting community.
* I understand that it may be a criminal offence or a breach of the school/setting policy to download or share inappropriate pictures, videos, or other material online. I understand that it is against the law to take, save or send nude or semi-nude images or videos 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.
* If, for any reason, I need to bring a personal device, for example a smart/mobile phone and/or other wearable technology into school/setting then I will…. **Insert expectations as according to individual school/setting policy decisions, for example, I know that it is to be kept on silent/off in my locker/bag during learning times or only used for educational purposes in class when approved by a member of staff.**
* I will respect other people’s information and copyright, for example, by giving a reference/source, ensuring any work submitted is my own, and asking permission before using images or text from online sources.
* I will always check that any information I create or 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 know it can be a criminal offence to gain unauthorised access to systems (‘hacking’), make, supply or obtain malware or send threatening and offensive messages.
* I will only change the settings on the computer if a teacher/technician has allowed me to.
* I know that use of the school/setting ICT system for personal financial gain, gambling, political purposes, or advertising is not allowed.
* I understand that the school/setting internet filter is there to protect me, and I will not try to bypass it.
* I know that if the school/setting 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.
* I know that if I do not follow the school/setting AUP then:
	+ **List sanctions.**
* 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.ceopeducation.co.uk](http://www.ceopeducation.co.uk), [www.childnet.com](http://www.childnet.com) and [www.childline.org.uk](http://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**

**Settings should amend and include specific information and expectations relating to their decisions relating to children’s use of devices and technology; for example, tablets, laptops, cloud computing, artificial intelligence (AI), shared file storage areas.**

**Learning**

* I know that school/setting 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 school/setting remote/online learning AUP. **If school/setting does not have a separate AUP, appropriate content should be included here.**
* I will only use my personal device/mobile phone in school/setting if I have permission from a teacher. **Other specific statements will be required if mobile phones/personal devices are or are not permitted**.

**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 school/setting devices and systems will be monitored, at home and at school, to protect me and to ensure I comply with the acceptable use policy. **Amend as appropriate to technology use by the age group, and to reflect your monitoring approaches.**
* 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 a share personal information and/or seek advice from an adult.
* I will keep my password safe and private as my privacy, school/setting 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 the school/setting 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/technician has allowed me to.
* I know that use of the school/setting ICT system for personal financial gain, gambling, political purposes, or advertising is not allowed.
* I understand that the school/setting internet filter is there to protect me, and I will not try to bypass it.
* I know that if the school/setting 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.
* I know that if I do not follow the school/setting AUP then:
	+ **List sanctions**

**Kind**

* I know that bullying in any form (on and offline) is not tolerated at school/setting name, and technology should not be used for harassment of any type.
* 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 school/setting 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 cybercrime can be a criminal offence, for example gaining unauthorised access to systems (‘hacking’) and making, supplying or obtaining malware.
* I know it can be a criminal offence to send threatening and offensive messages.
* I will respect other people’s information and copyright, for example, by giving a reference/source, ensuring any work submitted is my own, and asking permission before using images or text from online sources.
* I understand that it may be a criminal offence or breach of the school/setting 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.ceopeducation.co.uk](http://www.ceopeducation.co.uk), [www.childnet.com](http://www.childnet.com) and [www.childline.org.uk](http://www.childline.org.uk) to find out more about keeping safe online.
* I have read and talked about these expectations with my parents/carers.

**Shortened KS3/4 Version (for use on posters)**

**Responsible**

* I know I must respect the school/setting systems and equipment and if I cannot be responsible then I will lose the right to use them.
* I know that online content might not always be true.
* I know my online actions have offline consequences.
* I will always think before I post as text, photos or videos can become public, and impossible to delete once shared online.
* I will not use technology to be unkind to people.

**Private**

* I will keep my password and personal information private.
* I know I must always check my privacy settings are safe and private.

**Legal**

* I know that my internet use is monitored to protect me and ensure I comply with the school/setting acceptable use policy.
* I am aware that copyright laws exist, and I need to ask permission before using other people’s content and acknowledge any sources I use.
* I know cybercrime, such as hacking accounts or systems or sending abusive, threatening or offensive messages can be a criminal offence.

**Report**

* 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.
* If anything happens online which makes me feel worried or uncomfortable then I will speak to an adult I trust and visit [www.ceopeducation.co.uk](http://www.ceopeducation.co.uk).

### 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 school/setting rules then:
	+ **List sanctions.**

**Learners with SEND functioning at Levels P7-L1 (**[**Based on Childnet’s SMART Rules**](http://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 school/setting rules then:
	+ **List sanctions.**

**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**](http://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 school/setting rules then:
	+ - **List sanctions**

**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.

Pupil/Student Acceptable Use Policy Agreement Form

**If this form is appropriate and relevant (this will depend on the context of your learners, for example age and ability), settings should attach a copy of the appropriate version of their AUP to this form.**

**Settings may need to provide pupils/students and parents/carers with updated versions of the AUP as their children progress through the setting.**

**<School/College Name> Acceptable Use of Technology Policy – Child/Pupil/Student Agreement**

I, with my parents/carers, have read and understood the school/college Acceptable Use of Technology Policy (AUP) and remote learning AUP. **If separate**.

I agree to follow the AUP when:

1. I use school/college devices and systems (list as appropriate), both on site and at home.
2. I use my own devices in school/college when allowed, including mobile phones, smart technology, gaming devices, and cameras. **Amend in accordance with your mobile/smart technology policy**
3. I use my own equipment out of the school/college, including communicating with other members of the school/college or when accessing school/college systems. **Amend as appropriate.**

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

Class……………………………….………… Date…………………………………………….

Parent/Carer’s Name……………………………………………...………......... (**If appropriate**)

Parent/Carer’s Signature…………………………………………….…………. (**If appropriate**)

Date……………………………………………………………………………………………………

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

**We encourage schools/settings to provide a covering letter to parents/carers which explains the use of technology on and offsite if this is not addressed within the AUP or other communications: KCSIE states that schools and colleges should ensure parents/carers are aware of what their children are being asked to do online, including the sites they will asked to access and who from the school/college (if anyone) their child is going to be interacting with online.**

### Parent/Carer AUP Acknowledgement Form

**Settings should attach a copy of an age appropriate AUP that is relevant for the parent/carer to this form. Settings may need to provide parents/carers with updated versions of the AUP as children/pupils/students’ progress through the setting.**

**<Setting name> Child/Pupil/Student Acceptable Use of Technology Policy Acknowledgment**

1. I have read and discussed <setting name> child/pupil/student 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 school/setting devices and systems on site and at home including (list devices/systems), 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 child/pupil/student, could have repercussions for the orderly running of the school/setting, if a child/pupil/student is identifiable as a member of the school/setting, or if the behaviour could adversely affect the reputation of the school/setting.
3. I understand that any use of school/setting devices and systems are appropriately filtered; this means/includes… inset appropriate information about the filtering systems in place here. **KCSIE suggests that parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use.**
4. I am aware that my child’s use of school/setting provided devices and systems will be monitored for safety and security reasons, when used on and offsite. This includes… inset appropriate information about the monitoring systems in place here. **KCSIE suggests that parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use.** 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 the school/setting will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use school/setting devices and systems, on and offsite. I however understand that the school/setting 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. **Amend as appropriate to filtering/monitoring approaches implemented.**
6. I am aware that the school/setting mobile and smart technology policy states that my child can/cannot use personal devices, including mobile and smart technology on site. **Include specific details as outlined in your policy, for example, mobile phones should be handed to the office, kept switched off during lessons/on site.**
7. I understand that my child needs a safe and appropriate place to access remote/online learning, for example, if the school/setting 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/setting remote learning AUP. **Amend according to age/ability of children/pupils/students and setting remote/online learning decisions. Schools and colleges should ensure parents/carers are aware of what their children are being asked to do online, including the sites they will asked to access and who from the school/college (if anyone) their child is going to be interacting with online. If the setting does not use remote/online learning or have a separate remote/online learning AUP, appropriate content should be incorporated within the existing AUP.**
8. 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/setting community, or content that could adversely affect the reputation of the school/setting.
9. I understand that the school/setting will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child’s safety online.
10. I will inform the school/setting (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/setting community’s safety online. **Amend according to setting decisions, for example, make it clear if a class teacher/key worker/head of year should be the first point of contact.**
11. 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/setting.
12. I understand my role and responsibility in supporting the school/settings 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 ………………………………… **(If appropriate)**

Class……………………………………...………Date………………………………………………

Parent/Carer’s Name……………………………………………………………………………….......

Parent/Carer’s Signature………………………………………………………………...

Date…………………………….

### Sample Parent/Carer Acceptable Use of Technology Policy (AUP)

**If settings opt to use this approach, they should attach a copy of an age appropriate AUP to this form. Settings may need to provide parents with updated versions of the AUP as children progress through the setting.**

**Please be aware that issues for learning can be created if parents/carers refuse to agree an AUP before allowing access as children and young people will need to use the internet to access the curriculum. If settings opt to request parental consent before granting access to children, the setting should have a robust process in place to manage and record responses and to engage with parents/carers who do not respond or refuse to agree the AUP. Alternatives include highlighting online safety within the Home School Agreement and/or using an AUP acknowledgement form.**

1. I know that my child will be provided with internet access and will use a range of IT systems including **list as appropriate** in order to access the curriculum and be prepared for modern life whilst at < school/setting name>
2. I understand that the AUP applies to my child’s use of school/setting 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/student, could have repercussions for the orderly running of the school/setting, if a pupil/student is identifiable as a member of the school/setting, or if the behaviour could adversely affect the reputation of the school/setting.
3. I am aware that use of mobile and smart technology, such as mobile phones by children, is/is not permitted at <school/setting name> **Settings should add in specific information and expectations relating to management and use of children’s mobile technology on site.**
4. I understand that any use of school/setting devices and systems are appropriately filtered; this means/includes… inset appropriate information about the filtering systems in place here. **KCSIE suggests that parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use.**
5. I am aware that my child’s use of school/setting provided devices and systems will be monitored for safety and security reasons, when used on and offsite. This includes… inset appropriate information about the monitoring systems in place here. **KCSIE suggests that parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use.** 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.
6. I understand that the school/setting will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use school/setting devices and systems, on and offsite. I however understand that the school/setting 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. **Amend as appropriate to filtering/monitoring approaches implemented.**
7. 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/setting.
8. I have read and discussed < school/setting name> child/pupil/student Acceptable Use of Technology Policy (AUP) with my child.
9. I will support school/setting safeguarding policies and will ensure that I use appropriate parental controls, will appropriately supervise/monitor my child’s use of the internet outside of school/setting and will discuss online safety with them when they access technology at home.
10. I know I can seek support from the school/setting about online safety, such as via the school/setting website (link), to help keep my child safe online at home.
11. I will support the school/setting approach to online safety. I will role model safe and positive online behaviour for my child by sharing images, text, and video online responsibly.
12. I, together with my child, will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the school/setting community, or content that could adversely affect the reputation of the school/setting
13. I understand that a partnership approach to online safety is required. If the school/setting has any concerns about either my or my child’s behaviour or safety online, then I will be contacted.
14. I understand that if I or my child do not abide by the < school/setting name> AUP, appropriate action will be taken. This could include sanctions being applied in line with the school/setting policies (**list as appropriate**) and if a criminal offence has been committed, the police being contacted.
15. I know that I can speak to the Designated Safeguarding Lead (Name), my child’s class teacher/key worker/head of year or the headteacher/manager if I have any concerns about online safety.

**I have read, understood and agree to comply with the <setting name>** **Parent/Carer Acceptable Use of Technology Policy**.

Child’s Name……………………………………. Child’s Signature ………………………………… **(If appropriate)**

Class……………………………………...………Date………………………………………………

Parent/Carer’s Name……………………………………………………………………………….......

Parent/Carer’s Signature………………………………………………………………...

Date…………………………….

………………………………………………………………... Date…………………………….

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

### Staff Acceptable Use of Technology Policy (AUP)

**Amend as appropriate; this template is not exhaustive and should be adapted to reflect the decisions of the headteacher/manager and/or governing body/trustees/proprietor. Schools and settings, as well as individual members of staff, may wish to seek additional advice (such as HR/Personnel/Unions) as part of developing, implementing and agreeing with an AUP.**

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use < school/setting name > IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for children/pupils/students, 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 < school/setting name > expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that school/setting systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

**Policy scope**

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school/setting or accessed by me as part of my role within <school/setting name>, 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**. Amend as appropriate.**
2. I understand that < school/setting name> Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school/setting child protection/online safety policy **(amend as appropriate)**, staff behaviour policy/code of conduct and remote/online learning AUP. (**If not integrated within this 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/setting ethos, school/setting staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

**Use of school/setting** **devices and systems**

1. I will only use the equipment and internet services provided to me by the school/setting for example school/setting provided laptops, tablets, mobile phones and internet access, when working with children/pupils/students. **Amend as appropriate; if settings allow staff to use personal devices, clear boundaries and expectations should be detailed. Leaders should make informed decisions and be able to evidence their decision making.**
2. 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/is not allowed; (if allowed) this use at the school/setting’s discretion and can be revoked at any time. **Amend as appropriate; if settings allow staff to use work internet access/devices for personal use, clear boundaries should be detailed. Occasional personal use of the settings devices could be considered as beneficial to the development of staff IT skills and can enable staff to maintain a positive work-life balance. However, this is at the setting’s discretion and can be revoked at any time. Leaders should make informed decisions and be able to evidence their decision making.**
3. Where I deliver or support remote/online learning, I will comply with the school/setting remote/online learning AUP. **Remove this statement and add a separate section if you opt to integrate into the remote learning AUP.**

**Data and system security**

1. 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/setting systems. **A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system. Leaders should include any specific requirements, for example, how often passwords should be changed etc.**
	* I will protect the devices in my care from unapproved access or theft. **Detail how this should be achieved, for example not leaving devices visible or unsupervised in public places.**
2. I will respect school/setting system security and will not disclose my password or security information to others.
3. 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. **Amend as appropriate.**
4. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager. **Amend as appropriate.**
5. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK GDPR in line with the school/setting information security policies. **Amend as appropriate.**
	* 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/setting site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school/setting. **Amend and include specific details as appropriate.**
	* Any data being shared online, such as via cloud systems or artificial intelligence tools (AI), will be suitably risk assessed and approved by the school/setting Data Protection Officer and leadership team prior to use to ensure it is safe and legal. **Amend and include specific details as appropriate.**
6. I will not keep documents which contain school/setting related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school/setting learning platform to upload any work documents and files in a password protected environment or school/setting approved/provided VPN. **Amend as appropriate.**
7. I will not store any personal information on the school/setting IT system, including school/setting laptops or similar device issued to members of staff, that is unrelated to school/setting activities, such as personal photographs, files or financial information.
8. I will ensure that school/setting owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
9. I will not attempt to bypass any filtering and/or security systems put in place by the school/setting.
10. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Support Provider/Team/lead (named contact) as soon as possible.
11. If I have lost any school/setting related documents or files, I will report this to the ICT Support Provider/Team/lead (named contact) and school/setting Data Protection Officer (name) as soon as possible.
12. Any images or videos of children/pupils/students will only be used as stated in the school/setting camera and image use policy (link). I understand images of children/pupils/students must always be appropriate and should only be taken with school/setting provided equipment and only be taken/published where children/pupils/students and/or parent/carers have given explicit written consent.

**Classroom practice**

1. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by < school/setting name> as detailed in insert names of relevant policies, for example, child protection or online safety, and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training. **Leaders should ensure the online safety or child protection policy includes specific details for staff relating to regarding expectations, applicable roles and responsibilities for appropriate filtering and monitoring.**
2. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT provider/staff **(amend as appropriate)**, in line with the school/setting child protection/online safety policy. **Leaders should ensure this is detailed in the child protection or online safety policy. If this is not addressed in a separate policy, additional detail should be incorporated in this AUP.**
3. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in insert names of relevant policies, for example, child protection, online safety, remote learning AUP. **Leaders should ensure the AUP, online safety or child protection policy include specific details and expectations regarding safe practice relating to the specific use of technology, for example, use of specific platforms/search engines and AI tools. If not, this should be listed here.**
4. **Leaders should amend this section to reflect their individual decisions relating to use of AI and their school/setting specific context.** I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school/college 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/is not permitted by staff and pupils/students. (**amend as appropriate**)
	* A risk assessment will be undertaken, and written approval will be sought from the senior leadership team prior to any use of AI tools (for example if used in the classroom, or to support lesson planning or assessments). (**Remove if use of AI is not permitted**)
	* Any misuse of AI will be responded to in line with relevant school/college policies, including but not limited to, anti-bullying, staff and pupil/student behaviour and child protection. (**amend as appropriate, for example. reference any policies relating to exam/coursework etc.**)
5. I will promote online safety with the children/pupils/students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
	* exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
	* creating a safe environment where children/pupils/students 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) (name) or a deputy (names) as part of planning online safety lessons or activities to ensure support is in place for any children/pupils/students who may be impacted by the content.
	* Informing the DSL and/or leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
	* make informed decisions to ensure any online safety resources used with children/pupils/students is appropriate.
6. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

**Mobile devices and smart technology**

1. I have read and understood the school/setting mobile and smart technology and social media policies which addresses use by children/pupils/students and staff. **Amend policies listed as appropriate. Leaders should ensure a policy includes and addresses specific details and expectations regarding mobile and smart technology and use of social media. A template social media and mobile technology policy can be found** [**here**](https://www.theeducationpeople.org/our-expertise/partner-providers/kent-county-council-providers/safeguarding/template-policies-and-guidance/)**, or this can be addressed in the child protection/online safety policy.**
2. 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 behaviour policy/code of conduct and the school/setting mobile technology policy and the law. **Leaders should ensure there is a policy in place which addresses expectations regarding staff use of mobile devices/smart technology; a template social media and mobile technology policy can be found** [**here**](https://www.theeducationpeople.org/our-expertise/partner-providers/kent-county-council-providers/safeguarding/template-policies-and-guidance/)**. If this is not addressed in a separate policy, additional detail should be incorporated in this AUP, for example to state if mobile phones and personal devices are or are not permitted, including if they are only permitted within specific areas/ times or for specific tasks or circumstances.**

**Online communication, including use of social media**

1. 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/online safety policy, staff behaviour policy/code of conduct, social media policy and the law. **Amend as appropriate.**
2. As outlined in the staff behaviour policy/code of conduct and school/setting social media policy: **Amend as appropriate.**
	* I will take appropriate steps to protect myself and my reputation, and the reputation of the school/setting, online when using communication technology, including the use of social media.
	* I will not discuss or share data or information relating to children/pupils/students, staff, school/setting business or parents/carers on social media.

**Leaders should ensure there is a policy in place which addresses expectations regarding staff use of social media; a template social media policy can be found** [**here**](https://www.theeducationpeople.org/our-expertise/partner-providers/kent-county-council-providers/safeguarding/template-policies-and-guidance/)**. If this is not addressed in a separate policy, additional details and expectations should be incorporated in this AUP.**

1. My electronic communications with current and past children/pupils/students 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/setting approved and/or provided communication channels and systems, such as a school/setting email address, user account or telephone number.
	* I will not share any personal contact information or details with children/pupils/students, such as my personal email address or phone number.
	* I will not add or accept friend requests or communications on personal social media with current or past children/pupils/students and/or their parents/carers.
	* If I am approached online by a current or past children/pupils/students or parents/carers, I will not respond and will report the communication to my line manager and (name) Designated Safeguarding Lead (DSL).
	* Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL and/or headteacher/manager. **Amend as appropriate.**

**Policy concerns**

1. 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.
2. 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.
3. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school/setting into disrepute.
4. I will report and record any concerns about the welfare, safety or behaviour of children/pupils/students or parents/carers online to the DSL in line with the school/setting child protection policy.
5. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher/manager, in line with school/setting child protection policy and/or the allegations against staff policy. **Amend as appropriate.**

**Policy Compliance and Breaches**

1. If I have any queries or questions regarding safe and professional practise online, either in school/setting or off site, I will raise them with the DSL and/or the headteacher/manager.
2. I understand that the school/setting may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of children/pupils/students and staff. This includes monitoring all school/setting provided devices and school/setting systems and networks including school/setting provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school/setting provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
3. I understand that if the school/setting believe that unauthorised and/or inappropriate use of school/setting devices, systems or networks is taking place, the school/setting may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.
4. I understand that if the school/setting believe that unprofessional or inappropriate online activity, including behaviour which could bring the school/setting into disrepute, is taking place online, the school/setting may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.
5. I understand that if the school/setting suspects criminal offences have occurred, the police will be informed.

**I have read, understood and agreed to comply with <** **school/setting name> Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.**

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

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

Date (DDMMYY)……………………………………………………………………………………….…...

### Visitor and Volunteer Acceptable Use of Technology Policy

**This template should be amended according to the visitor type; visitors who are provided with access to school/setting devices and systems may require a different AUP to those who are not permitted any access.**

As a professional organisation with responsibility for safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of our behaviour expectations and their professional responsibilities when using technology. This AUP will help < school/setting name> ensure that all visitors and volunteers understand the school/settings expectations regarding safe and responsible technology use.

**Policy scope**

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school/setting or accessed by me as part of my role within <school/setting name>, professionally and personally. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email. data and data storage, remote learning systems and communication technologies**. Amend as appropriate.**
2. I understand that < school/setting name> AUP should be read and followed in line with the school/setting staff behaviour policy/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/setting ethos, school/setting staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.
4. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.
5. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.
6. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school/setting into disrepute.

**Data and image use**

1. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including UK GDPR. **This statement is only required if visitors/volunteers have access to school/setting data.**
2. I understand that I am/am not allowed to take images or videos of children/pupils/students. **Amend as appropriate**. Any images or videos of children/pupils/students will only be taken in line with the school/setting camera and image use policy (link). **Remove if visitors/volunteers are not allowed to take mages/videos.**

**Classroom practice**

1. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of children/pupils/students. **Remove if visitors/volunteers will not be supporting learning. Leaders should include specific details and expectations regarding safe classroom practice or signpost to appropriate policies.**
2. Where I deliver or support remote/online learning, I will comply with the school/setting remote/online learning AUP. **Remove if visitors/volunteers will not support remote/online learning. Settings will need to remove this statement and add a separate section if they opt to integrate the remote/online learning AUP.**
3. I will support and reinforce safe behaviour whenever technology is used on site, and I will promote online safety with the children/pupils/students in my care.
4. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the school/setting community, I will report this to the DSL and IT provider/staff **(amend as appropriate)**, in line with the school/setting child protection/online safety policy. **Leaders should ensure this is detailed in the child protection or online safety policy. If this is not addressed in a separate policy, additional detail should be incorporated in this AUP.**
5. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them. **Amend as appropriate to the role of the visitor/volunteer.**

**Use of mobile devices and smart technology**

1. In line with the school/setting mobile and smart technology policy, I understand that.... **List details regarding settings expectations regarding visitor use of mobile devices and smart technology, for example, mobile phones and personal devices are not permitted or are only permitted within specific areas etc. Leaders should ensure policies include specific details and expectations regarding visitors use of mobile technology; a template social media and mobile technology policy can be found** [**here**](https://www.theeducationpeople.org/our-expertise/partner-providers/kent-county-council-providers/safeguarding/template-policies-and-guidance/)**.**

**Online communication, including the use of social media**

1. I will ensure that my online reputation and use of technology and is compatible with my role within the school/setting.  This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
	* I will take appropriate steps to protect myself online as outlined in the child protection/online safety/social media policy (link). **Amend as appropriate.**
	* I will not discuss or share data or information relating to children/pupils/students, 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/setting code of conduct/behaviour policy and the law.
2. My electronic communications with children/pupils/students, 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/setting approved communication channels such as via a school/setting provided email address, account or telephone number.
	* Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
	* Any pre-existing relationships or situations that may compromise my ability to comply with this will be discussed with the DSL (name) and/or headteacher/manager.

**Policy compliance, breaches or concerns**

1. If I have any queries or questions regarding safe and professional practice online either in school/setting or off site, I will raise them with the Designated Safeguarding Lead (name) and/or the headteacher/manager.
2. I understand that the school/setting may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of children/pupils/students and staff. This includes monitoring all school/setting provided devices and school/setting systems and networks including school/setting provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school/setting provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation. **Only required if visitors/volunteers will have access to school/setting devices and systems.**
3. I will report and record concerns about the welfare, safety or behaviour of children/pupils/students or parents/carers online to the Designated Safeguarding Lead (name) in line with the school/setting child protection policy.
4. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher/manager, in line with the allegations against staff policy.
5. I understand that if the school/setting believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school/setting may invoke its disciplinary procedures.
6. I understand that if the school/setting suspects criminal offences have occurred, the police will be informed.

**I have read, understood and agreed to comply with <** **school/setting name> visitor/volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.**

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

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

Date (DDMMYY)………………………………………………............................................................................

### Wi-Fi Acceptable Use Policy

**This template is for schools and settings who provide Wi-Fi internet access to guest users; this may include children/young people, visitors and volunteers and/or staff using personal devices.**

**Settings may wish to use a paper or electronic AUP for guest access of Wi-Fi by members of the community. This template is provided for settings to adapt and use as appropriate.**

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

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

1. The school/setting provides Wi-Fi for the school/setting community and allows access for (**state purpose, for example education use only). Settings should include any include information about time limits, passwords, and security.**
2. I am aware that the school/setting will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school/setting takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the school/setting premises that is not the property of the school/setting.
3. The use of technology falls under <setting name> Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy (**any other relevant policies such as data security, child protection, online safety**) which all children/pupils/students /staff/visitors and volunteers must agree to and comply with.
4. The school/setting reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.
5. School/setting owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
6. I will take all practical steps necessary to make sure that any equipment connected to the school/setting service is adequately secure, such as up-to-date anti-virus software, systems updates.
7. The school/setting wireless service is not secure, and the school/setting cannot guarantee the safety of traffic across it. Use of the school/setting wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.
8. The school/setting accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school/setting wireless service’s connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school/setting from any such damage.
9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.
10. I will not attempt to bypass any of the school/setting security and filtering systems or download any unauthorised software or applications.
11. My use of school/setting Wi-Fi will be safe and responsible and will always be in accordance with the school/setting AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school/setting into disrepute.
13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (name) as soon as possible.
14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (name) or the headteacher/manager.
15. I understand that my use of the school/setting Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school/setting suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school/setting may terminate or restrict usage. If the school/setting suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

**I have read, understood and agreed to comply with <school/setting name> Wi-Fi Acceptable Use Policy.**

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

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

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

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

**KCSIE states “*Schools and colleges are likely to be in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online”.***

**These templates specifically address safer practice when running formal remote/online learning, including live streamed sessions, but can also apply to other online communication, such as remote/online parent meetings or pastoral activities. Settings should implement the approaches that best suit the needs of their community following appropriate discussions.**

**A remote/online learning AUP should be implemented following a thorough evaluation of remote/online 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 children, young people and/or parents/carers.**

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

* LGfL: [Safeguarding Considerations for Remote Learning](https://lgfl.net/safeguarding/safe-remote-learning)
* SWGfL: [Which Video Conference platform is best?](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:
		- [Online Safety Guidance for the Full Opening of Schools](https://www.kelsi.org.uk/__data/assets/pdf_file/0014/110606/Online-Safety-Guidance-for-the-Full-Opening-of-Schools.pdf)
	+ The Education People: [Covid-19 Specific Safeguarding Guidance and Resources](https://www.theeducationpeople.org/our-expertise/safeguarding/template-policies-and-guidance/)
		- [‘Safer remote learning during Covid-19: Information for School Leaders and DSLs’](https://www.theeducationpeople.org/blog/safer-remote-learning-during-covid-19-information-for-school-leaders-and-dsls/)
* National guidance:
	+ DfE: ‘[Safeguarding and remote education during coronavirus (COVID-19)](https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19)
	+ SWGfL: [Safer Remote Learning](https://swgfl.org.uk/resources/safe-remote-learning/)
	+ NSPCC: [Undertaking remote teaching safely](https://learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely)
	+ Safer Recruitment Consortium: [Guidance for safer working practice](https://saferrecruitmentconsortium.org/)

### Remote/Online Learning AUP Template - Staff Statements

**These statements can be incorporated as appropriate within your existing staff AUP if preferred. Supply staff or online tutors employed by the school/setting should agree and follow your child protection policy, staff behaviour policy and associated AUPs.**

**<School/setting Name> Staff Remote/Online Learning AUP**

The Remote/Online Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of school/setting name community when taking part in remote/online learning, for example following any full or partial school/setting closures.

**Leadership oversight and approval**

1. Remote/online learning will only take place using system name(s).
	* System name has been assessed and approved by the headteacher/a member of Senior Leadership Team (SLT). **The guidance notes section links to organisations/tools which can support leaders in making informed decisions and selecting appropriate platforms.**
2. Staff will only use school/setting managed or specific, approved professional accounts with children/pupils/students **and/or** parents/carers. **It is recommended staff use school/setting managed systems where possible or are required to set up separate school/school approved professional accounts.**
	* Use of any personal accounts to communicate with children/pupils/students and/or parents/carers is not permitted.
		+ Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with name, Designated Safeguarding Lead (DSL).
	* Staff will use work provided equipment where possible**,** for example, a school/setting laptop, tablet, or other mobile device. **If this is not provided, leaders should ensure clear expectations are in place in relation to safeguarding and data security when using personal devices, for example, using strong passwords, suitable levels of encryption, logging off or locking devices when not in use etc.**
3. Online contact with children/pupils/students **and/or** parents/carers will not take place outside of the operating times as defined by SLT:
	* Insert agreed times.
4. All remote/online lessons will be formally timetabled**; a member of SLT, DSL and/or head of department is** able to drop in at any time. **Amend as appropriate to system and SLT decision.**
5. Live-streamed remote/online learning sessions will only be held with approval and agreement from the headteacher/a member of SLT. **Remove/amend as appropriate to system and SLT decision.**

**Data Protection and Security**

1. Any personal data used by staff and captured by system name when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy (link).
	* **Only needed if personal data will be used/stored. If so, detail specifics of how this will be achieved, for example, using bcc to email multiple users. Schools and colleges should continue to follow the guidance outlined in the**[**data protection: toolkit for schools**](https://www.gov.uk/government/publications/data-protection-toolkit-for-schools)**when managing personal data.**
2. All remote/online learning and any other online communication will take place in line with current school/setting confidentiality expectations as outlined in xxxx policy. **Amend as appropriate.**
	* **List specific expectations if required, taking platform safety/security issues as appropriate into account.**
3. All participants will be made aware that system namerecords activity. **Only needed if the session is recorded by the system: settings should amend as appropriate to the approach and system being used. Please note, consent from those involved in the session is required if settings are recording activity. Settings should be clear about how recordings will be stored, how long they will be kept for and who will have access to them, in line with your existing data protection policy.**
4. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements. **Remove if this is not permitted under any circumstance.**
5. Only members of the <School/Setting name> community will be given access to system name.
6. Access to system name will be managed in line with current IT security expectations as outlined in policy name.
	* **If not covered in a different policy, settings should detail specific expectations, for example, using strong passwords, logging off or locking devices when not in use etc.**

**Session management**

**Note: Not all statements will be needed if settings are not delivering live content**

1. Staff will record the length, time, date, and attendance of any sessions held. **Detail how and where this information should be stored.**
2. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
	* **Detail specifics according to the system being used, for example, language filters, disabling/limiting chat, staff not permitting children/young people to share screens, keeping meeting IDs private, use of waiting rooms/lobbies or equivalent.**
3. When live streaming with children/pupils/students: **Remove if not live streaming with children/young people.**

**I have read and understood <** **school/setting name> Video Conferencing and/or Live Communication Acceptable Use Policy (AUP).**

**Learner/Parent/Carer**

Child’s Name……………………………………………………………………………………………...

Class…………………………

Parent/Carers: ……………………………………………......................................................

Date (DDMMYY)………………………………………………...

**Staff**

Name: …………………………………………………………………………………………………

Date (DDMMYY)………………………………………………...

* + contact will be made via children’s/pupils/students **school/setting** provided email accounts **and/or** logins. **Amend as appropriate.**
	+ contact will be made via a parents/carers account. **Remove if not live-streaming with children/young people or if this not necessary. Some platforms have age restrictions which prevent them being used with children. his statement is unlikely to be required if children/young people are using internally managed systems.**
	+ staff will mute/disable children’s/pupils/students’ videos and microphones. **Amend as appropriate to system and SLT decision, for example, if video/microphones should be muted throughout or if they will be allowed under staff control at specific times. This is likely to vary based on age and ability of children/pupils/students.**
	+ at least 2 members of staff will be present. **Amend as appropriate to system and SLT decision.**
		- If this is not possible, SLT approval will be sought.
1. Live 1:1 sessions will only take place with approval from the headteacher/a member of SLT. **Remove if not permitted at all. Live** **1:1 sessions with children/pupils/students are not recommended unless they are approved by SLT, a parent/carer is present in the room if possible (however, this may not be appropriate if providing counselling or safeguarding support) and the session is auditable.**
2. A pre-agreed invitation/email (**as relevant to system being used)** detailing the session expectations will be sent to those invited to attend.
	* Access links should not be made public or shared by participants. **If relevant to system being used.**
	* Children/pupils/students **and/or** parents/carers should not forward or share access links.
	* If children/pupils/students or parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first. **Amend as appropriate.**
	* Children/pupils/students 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. **Amend as appropriate.**
3. Alternative approaches and/or access will be provided to those who do not have access. **Amend as appropriate to options available, for example, if settings will loan devices etc.**

 **Behaviour expectations**

1. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
2. All participants are expected to behave in line with existing school/setting policies and expectations. This includes **Detail specific expectations as appropriate to setting decisions. Examples could include:**
	* **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.**

1. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
2. When sharing videos and/or live streaming, participants are required to: **Remove if not sharing videos or live-streaming. Amend as appropriate to system and SLT decision. Examples could include:**
	* **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.**
3. 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**

1. Participants are encouraged to report concerns during remote and/or live-streamed sessions:
	* Insert specifics or reference where to find them. **For children/pupils/students, schools could insert age/ability appropriate details, for example, reporting concerns to the member of staff running the session, telling a parent/carer etc.**
2. 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 name and role.
3. 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.
4. Sanctions for deliberate misuse may include **Insert details, for example, restricting/removing use, contacting police if a criminal offence has been committed.**
5. Any safeguarding concerns will be reported to **name**, Designated Safeguarding Lead, in line with our child protection policy.

### Remote/Online Learning AUP Template – Pupil/Student Statements

**I have read and understood the <school/setting name>** **Acceptable Use Policy (AUP) for remote/online learning.**

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

Date………………………………………………………………………………………………………………….

**These statements can be incorporated as appropriate within your existing learner AUP if preferred. This AUP is initially aimed at pupils/students in KS3/4+; settings will need to amend the content according to their pupils/students age and ability and relevant leadership decisions.**

**<School/setting Name> Pupil/Student Remote/Online Learning AUP**

1. I understand that:
	* these expectations are in place to help keep me safe when I am learning at home using **system name, for example, Microsoft Teams, Google Meet etc**.
	* I should read and talk about these rules with my parents/carers.
	* remote/online learning will only take place using **system name(s)** and during usual **school/setting** times.
	* my use of **system name** is monitored to help keep me safe. **Please note, if settings are recording activity taking place during remote/online learning, consent from those involved is required. Settings should be clear about how recordings will be stored, how long they will be kept for and who will have access to them, in line with your existing data protection policy.**
2. Only members of the <**School/Setting name**> community can access **system name**.
	* I will onlyuse my **school/setting** provided email accounts **and/or** login to access remote learning. **Amend as appropriate.**
	* 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/online learning I will behave as I would in the classroom. This includes **Detail specific expectations as appropriate to setting decisions and pupils/students age/ability. Examples could include:**
	* **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: **Amend as appropriate to system and SLT decisions; remove this section if live streaming is not taking place.**

**I have read and understood <** **school/setting name> Video Conferencing and/or Live Communication Acceptable Use Policy (AUP).**

**Learner/Parent/Carer**

Child’s Name……………………………………………………………………………………………...

Class…………………………

Parent/Carers: ……………………………………………......................................................

Date (DDMMYY)………………………………………………...

**Staff**

Name: …………………………………………………………………………………………………

Date (DDMMYY)………………………………………………...

* + mute my video and microphone. **Amend as appropriate to system and SLT decision, for example, if pupils/students’ video/microphones should be muted throughout or if they will be allowed under staff control at specific times. This is likely to vary based on age and ability of pupils/students.**
	+ wear appropriate clothing and be in a suitable location. **Remove if pupil/student videos are disabled.**
	+ ensure backgrounds of videos are neutral and personal information/content is not visible. **Remove if pupil/student videos are disabled.**
	+ use appropriate alternative backgrounds. **Remove if pupil/student videos are disabled. Amend as appropriate to system and SLT decision**
	+ 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. **Amend as appropriate to age/ability of children/pupil/student.**
1. If I am concerned about anything that takes place during remote/online learning, I will:
	* **insert age/ability appropriate details, for example, reporting concerns to the member of staff running the session, tell a parent/carer etc.**
2. I understand that inappropriate online behaviour or concerns about my or others safety during remote/online learning will be taken seriously. This could include:
	* **Insert details, for example, restricting/removing access, informing parents/carers, contacting police if a criminal offence has been committed.**

**I have read and understood the <school/setting name>** **Pupil/Student** **Acceptable Use Policy (AUP) for remote learning.**

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

Class…………………………………...…………. Date……………………………………….……….

Parent/Carer’s Name………………………………...…………………………........ (***If appropriate***)

Parent/Carer’s Signature……………………………………….……………………. (***If appropriate***)

Date……………………………………………………………………………………………….……….

# 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.