

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



Disclaimer

The Kent County Council LADO Education Safeguarding Advisory Service makes every effort to ensure that the information in our templates is accurate and up to date, however, ultimate responsibility for ensuring their individual policies are appropriate remains the responsibility of the school/college/setting leadership team. 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, schools/colleges, early years settings or other education settings that work with children 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.

Contents

Using the AUP Templates: Guidance Notes	3
Child/Pupil/Student Acceptable Use of Technology Sample Statements	5
Early Years and Key Stage 1 (0-6).....	5
Key Stage 2 (7-11)	6
Key Stage 3/4/5 (11-18).....	7
Children/Pupils/Students with Special Educational Needs and Disabilities (SEND)	Error!
Bookmark not defined.	
Acceptable Use of Technology Sample Statements and Forms for Parents/Carers	8
Parent/Carer AUP Acknowledgement Form	8
Sample Parent/Carer Acceptable Use of Technology Policy (AUP)	Error! Bookmark not defined.
Acceptable Use of Technology for Staff, Visitors and Volunteers Sample Statements	10
Staff Acceptable Use of Technology Policy (AUP)	10
Visitor and Volunteer Acceptable Use of Technology Policy	16
Wi-Fi Acceptable Use Policy.....	19
Template Acceptable Use Policy (AUP) for Remote/Online Learning	20
Remote/Online Learning AUP Template - Staff Statements.....	21
Remote/Online Learning AUP Template – Pupil/Student Statements	23
Acknowledgements and Thanks	25

Using these Templates: Guidance Notes

[‘Keeping Children Safe in Education’](#) (KCSIE) states that schools and colleges should have a ‘*staff behaviour policy (sometimes called the code of conduct) which should, amongst other things, include acceptable use of technologies, staff/pupil relationships and communications including the use of social media*’.

This document will support education 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.
- Additional content or changes for 2025-26 have been **highlighted in yellow**.

Using these Templates: Guidance Notes

Leaders, managers and DSLs should adapt the content in these templates to include specific local information, procedures and expectations. These details will vary from setting to setting, based on decisions by individual school leaders, 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 the needs of individual provisions.

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

Filtering and Monitoring

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

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

Use of Artificial Intelligence

Generative artificial intelligence (AI) tools have many uses which could benefit education settings. However, it is also important to recognise that AI tools can 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 leaders will need to make informed decisions regarding whether/how AI is permitted/used within their community. Where settings do permit use, we recommend these templates are adapted to reflect your specific expectations for use by staff and pupils/students as appropriate.

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

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

Child/Pupil/Student Acceptable Use of

Early Years and Key Stage 1 (0-6)

- I understand that the school rules will help keep me safe and happy when I go online.
- I only go online when a grown-up is with me.
- I only click on online things online when I know what they do. If I am not sure, I ask a grown-up first.
- I keep my personal information and passwords safe.
- I only send polite and friendly messages online.
- I know the school can see what I am doing online when I use school computers/tablets or use school software programmes
- If I see something online that makes me feel upset, unhappy, or worried I will always tell an grown-up .
- I can visit www.ceopeducation.co.uk (include other age-appropriate links) to learn more about keeping safe online.
- 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 Acceptable Use Policy will help keep me safe and happy online at home and at school

Safe

- I will be kind and respectful online, just like I am in school.
- I only send messages which are polite and friendly.
- I will only share pictures or videos online if they are safe, kind, and I have asked for permission first.
- I will only click on links if a trusted adult says they are safe.
- I know that people online might not be who they say they are. I will only chat with people I know or who a trusted adult says are safe.
- If someone online asks to meet me, I will tell a trusted adult straight away.

Learning

- I always ask permission from an adult before using the internet.
- I only use websites, tools and/or search engines that my teacher has chosen or given me permission to use.
- I use school devices for school work unless I have permission otherwise.
- If I need to learn online at home, I will follow the same rules in this policy.

Trust

- I know that some things or people online might not be honest or truthful.
- If I'm not sure something online is true, I will check with other websites, books, or ask a trusted adult.
- I always credit the person or source that created any work, images, or text I use.
- I will use Artificial Intelligence (AI) tools safely and sensibly. I won't use them to cheat, copy other people's work, or say anything unkind. I know that AI tools can sometimes make mistakes. I will only use them when a teacher or trusted adult says it's okay.

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 makes me feel worried or upset, I will 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 an adult at school.
- I know it is not my fault if I see something upsetting or unkind online.
- If I'm not sure about something online or it makes me feel worried or scared, I will talk to a trusted adult.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all school owned devices and networks are checked/monitored to help keep me safe, even if I use them at home. This means someone at the school may be able to see and/or check my online activity when I use school devices and/or networks if they are worried about my or anyone else's safety or behaviour.
- If, for any reason, I need to bring a personal device, like a smart/mobile phone and/or other wearable technology into school/setting **then 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 and www.childline.org.uk to learn more about being safe online or to see help.
-

Shortened KS2 version (for use on posters)

- I ask an 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 devices and systems can be monitored.

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

Parent/Carer AUP Acknowledgement Form

St Katharine's Knockholt Child Acceptable Use of Technology Policy Acknowledgment

1. I have read and discussed **St Katharine's Knockholt Child 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 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 child, could have repercussions for the orderly running of the school, if a child is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.
3. I understand that any use of school devices and systems are appropriately filtered.
4. I am aware that my child's use of school provided devices and systems will be monitored for safety and security reasons, when used on and offsite. Monitoring approaches are in place to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
5. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use school devices and systems, on and offsite. I however understand that the school cannot ultimately be held responsible for filtering breaches that occur due to the dynamic nature of materials accessed online, or if my child is using a personal device, including mobile or smart technologies. **Personal Devices are not allowed.**
6. I am aware that the school mobile and smart technology policy states that my child cannot use personal devices, including mobile and smart technology on site. **Mobile phones should be handed to the office.**
7. I understand that my child needs a safe and appropriate place to access remote/online learning, for example, if the **school is** closed. I will ensure my child's access to remote/online learning is appropriately supervised and any use is in accordance with the

school remote learning AUP.

- 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 community, or content that could adversely affect the reputation of the school .
- 9. I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety online.
- 10. I will inform the school (for example speaking to a member of staff and/or the Designated Safeguarding Lead) or other relevant organisations if I have concerns over my child's or other members of the school community's safety online.
- 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 .
- 12. I understand my role and responsibility in supporting the school 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.....		

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

Staff Acceptable Use of Technology Policy (AUP)

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

Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school or accessed by me as part of my role within St Katharine's, professionally and personally, both on and offsite. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email, data and data storage, remote learning systems and communication technologies.
2. I understand that St Katharine's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school child protection/online safety policy **and** staff behaviour policy/code of conduct
3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school ethos, staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of school devices and systems

4. I will only use the equipment and internet services provided to me by the school for example school provided laptops, tablets, mobile phones and internet access, when working with children .
5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff.
6. Where I deliver or support remote/online learning, I will comply with the school remote/online learning AUP.

Data and system security

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
 - I will use a 'strong' password to access school systems.
 - I will protect the devices in my care from unapproved access or theft
8. I will respect school system security and will not disclose my password or security information to others.
9. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the school office
10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.
11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK GDPR in line with the school information security policies.
 - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
 - Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school .
 - 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 Data Protection Officer and leadership team prior to use to ensure it is safe and legal.
12. I will not keep documents which contain school related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school learning platform to upload any work documents and files in a password protected environment or school [approved](#) VPN.

13. I will not store any personal information on the school IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.
14. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
15. I will not attempt to bypass any filtering and/or security systems put in place by the school .
16. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the school trip as soon as possible.
17. If I have lost any school related documents or files, I will report this to the school office and school Data Protection Officer (Sarah Jane Tormey) as soon as possible.
18. Any images or videos of children will only be used as stated in the school camera and image use policy (link). I understand images of children must always be appropriate and should only be taken with school provided equipment and only be taken/published where children/ and/or parent/carers have given explicit written consent.

Classroom practice

19. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by St Katharine's as detailed in child protection or online safety, and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.
20. 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 school office in line with the school child protection/online safety policy. .
21. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in child protection, online safety, remote learning AUP.
22. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I also recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material. Additionally, its use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that:
 - o AI tools are only to be used responsibly and ethically, and in line with our school child protection, data protection, and professional conduct/behaviour policy expectations.

- 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.
- A Data Protection Impact Assessment (DPIA) will always be completed prior to any use of AI tools that may be processing any personal, sensitive or confidential data and use will only occur following approval from the DPO.
- I am required to critically evaluate any AI-generated content for accuracy, bias, and appropriateness before sharing or using it in educational contexts.
- AI must not be used to replace professional judgement, especially in safeguarding, assessment, or decision-making involving children .
- Only approved AI platforms may be used with children . Children must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
- 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. (.

23. I will promote online safety with the children 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 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) (Sarah Jane Tormey) or a deputy (Xanthe Venezianni or Jo Botley) as part of planning online safety lessons or activities to ensure support is in place for any children 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 is appropriate.

24. 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

25. I have read and understood the school mobile and smart technology and social media policies which addresses use by children and staff.
26. 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 mobile technology policy and the law..

Online communication, including use of social media

27. 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. .
28. As outlined in the staff behaviour policy/code of conduct and school/setting social media policy:
- I will take appropriate steps to protect myself and my reputation, and the reputation of the school/ online when using communication technology, including the use of social media.
 - I will not discuss or share data or information relating to children , staff, school business or parents/carers on social media.
29. My electronic communications with current and past children and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
- I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels and systems, such as a school email address, user account or telephone number.
 - I will not share any personal contact information or details with children , 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 and/or their parents/carers.
 - If I am approached online by a current or past children or parents/carers, I will not respond and will report the communication to my line manager and Sarah Jane Tormey (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 .

Policy concerns

30. 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.
31. 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.
32. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

- 33. I will report and record any concerns about the welfare, safety or behaviour of children or parents/carers online to the DSL in line with the school child protection policy.
- 34. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with school child protection policy and the allegations against staff policy.

Policy Compliance and Breaches

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

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

Name of staff member:

Signed:

Date (DDMMYY).....

Visitor and Volunteer Acceptable Use of Technology Policy

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

Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school or accessed by me as part of my role within St Katharine's 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.
2. I understand that St Katharine's AUP should be read and followed in line with the school 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 ethos, school 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 into disrepute.

Data and image use

7. I understand that I **am not allowed to take images or videos of children..**

Classroom practice

8. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces.

9. I will support and reinforce safe behaviour whenever technology is used on site, and I will promote online safety with the children in my care.
10. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the school community, I will report this to the DSL and IT staff in line with the school/ child protection/online safety policy. .
11. 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.

Use of mobile devices and smart technology

12. In line with the school mobile and smart technology policy, I understand that mobile phones are not to be used in areas where children are present and should only be used in the staffroom or office areas.

Online communication, including the use of social media

13. I will ensure that my online reputation and use of technology and is compatible with my role within the school . This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
 - I will take appropriate steps to protect myself online as outlined in the child protection/online safety/social media policy.
 - I will not discuss or share data or information relating to children , staff, school 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.
14. My electronic communications with children/ , parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
 - All communication will take place via school approved communication channels such as via a school provided email address, account or telephone number.
 - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
 - Any pre-existing relationships or situations that may compromise my ability to comply with this will be discussed with the DSL (Sarah Jane Tormey) and/or headteacher/manager.

Policy compliance, breaches or concerns

15. If I have any queries or questions regarding safe and professional practice online either in school or off site, I will raise them with the Designated Safeguarding Lead (Sarah Jane Tormey) and/or the headteacher/manager.

- 16. I understand that the school may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of children and staff. This includes monitoring all school provided devices and school systems and networks including school provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation. .
- 17. I will report and record concerns about the welfare, safety or behaviour of children or parents/carers online to the Designated Safeguarding Lead (Sarah Jane Tormey) in line with the school child protection policy.
- 18. 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.
- 19. I understand that if the school believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.
- 20. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with St Katharine’s visitor/volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer:

Signed:

Date (DDMMYY).....

Wi-Fi Acceptable Use Policy

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

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

1. The school provides Wi-Fi for the school community and allows access for guest access only
2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the school premises that is not the property of the school .
3. The use of technology falls under St Katharine's 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 /staff/visitors and volunteers must agree to and comply with.
4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.
5. School owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
6. I will take all practical steps necessary to make sure that any equipment connected to the school service is adequately secure, such as up-to-date anti-virus software, systems updates.
7. The school wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.
8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.
10. I will not attempt to bypass any of the school security and filtering systems or download any unauthorised software or applications.
11. My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.
13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Sarah Jane Tormey) as soon as possible.
14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (Sarah Jane Tormey) or the headteacher/manager.
15. I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agreed to comply with St Katharine’s Wi-Fi Acceptable Use Policy.

Name

Signed:Date (DDMMYY).....

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

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 be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online”.

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

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

- LGfL: [Safeguarding Considerations for Remote Learning](#)
- SWGfL: [Which Video Conference platform is best?](#)

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

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

Remote/Online Learning AUP Template - Staff Statements

St Katharine’s Staff Remote/Online Learning AUP

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

Leadership oversight and approval

1. Remote/online learning will only take place using TEAMS
 - Teams has been assessed and approved by the headteacher/
2. Staff will only use school managed or specific, approved professional accounts with children/ **and/or** parents/carers.
 - Use of any personal accounts to communicate with children and/or parents/carers is not permitted.
 - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with Sarah Jane Tormey, Designated Safeguarding Lead (DSL).
 - Staff will use work provided equipment where possible, for example, a school/setting laptop, tablet, or other mobile device.
3. Online contact with children **and/or** parents/carers will not take place outside of the operating times as defined by SLT:
 - 8.30 am to 4.30pm.
4. All remote/online lessons will be formally timetabled; **a member of SLT, DSL and/or headteacher** is able to drop in at any time.
5. Live-streamed remote/online learning sessions will only be held with approval and agreement from the headteacher .
6.
Data Protection and Security
 -
7. All remote/online learning and any other online communication will take place in line with current school confidentiality
8. All participants will be made aware that Teams can record activity.
9. Only members of the St Katharine's community will be given access to Teams.
 -
10. Staff will record the length, time, date, and attendance of any sessions held.
11. Appropriate privacy and safety settings will be used to manage access and interactions.

12. A pre-agreed invitation/email detailing the session expectations will be sent to those invited to attend.
- Access links should not be made public or shared by participants.
 - Children parents/carers should not forward or share access links.
 - Children 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.
13. Alternative approaches and/or access will be provided to those who do not have access.
School may be able to loan devices.

Behaviour expectations

14. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
15. All participants are expected to behave in line with existing school/setting policies and expectations.
16. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
17. When sharing videos and/or live streaming, participants are required to:
- **wear appropriate dress.**
 - **ensure backgrounds of videos are neutral (blurred if possible).**
 - **ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.**
18. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

19. Participants are encouraged to report concerns during remote and/or live-streamed sessions:
20. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to a headteacher.
21. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.
22. Any safeguarding concerns will be reported Sarah Jane Tormey, Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the [St Katharine's](#) Acceptable Use Policy (AUP) for remote/online learning.

Staff Member Name:

Remote/Online Learning AUP Template – Pupil/Student Statements

St Katharine’s 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 **Microsoft Teams etc.**
 - I should read and talk about these rules with my parents/carers.
 - remote/online learning will only take place using **Teams** and during usual **school/setting** times.
 - my use of **Teams** is monitored to help keep me safe.

2. Only members of the St Katharine’s community can access **Teams**.
 - I will only use my **school** provided email accounts **and** login to access remote learning. .
 - I will use privacy settings as **agreed with my teacher** .
 - 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.

4. When taking part in live sessions I will:
 - mute my video and microphone. .
 - wear appropriate clothing and be in a suitable location.
 - ensure backgrounds of videos are neutral and personal information/content is not visible. .
 - use appropriate alternative backgrounds.
 - attend the session in full. If for any reason I cannot attend a session in full, I will let my teacher know.
 - attend lessons in a shared/communal space or room with an open door and/or where possible when I can be supervised by a parent/carer or another appropriate adult.

5. If I am concerned about anything that takes place during remote/online learning, I will:
 - Tell my teacher and my parent/carer

6. I understand that inappropriate online behaviour or concerns about my or others safety during remote/online learning will be taken seriously.

I have read and understood the St Katharine’s Acceptable Use Policy (AUP) for remote learning.

Name..... Signed.....

Class..... Date.....

Acknowledgements and Thanks

This document has been produced by LADO Education Safeguarding Advisory 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.