

Acceptable Use of Technology Policy Templates

for Schools and Education Settings

KEEPING CHILDREN SAFE IN THE CHILDREN'S WORKFORCE

Contents

Guidance Notes ..... Error! Bookmark not defined.
Key Considerations ..... **Error! Bookmark not defined.**
Using this document ..... **Error! Bookmark not defined.**
Filtering and Monitoring ..... **Error! Bookmark not defined.**
Mobile Phones and Screen Use ..... **Error! Bookmark not defined.**
Use of Artificial Intelligence (AI) ..... **Error! Bookmark not defined.**
Social Media ..... **Error! Bookmark not defined.**
Disclaimer and Copyright ..... **Error! Bookmark not defined.**
Child/Pupil/Student Acceptable Use of Technology Sample Statements 3
Early Years and Key Stage 1 (0-6) 3
Key Stage 2 (7-11) 4
Children/Pupils/Students with Special Educational Needs and Disabilities (SEND) 7
Acceptable Use of Technology Sample Statements and Forms for Parents/Carers 9
Parent/Carer AUP Acknowledgement Form ..... **Error! Bookmark not defined.**
Sample Parent/Carer Acceptable Use of Technology Policy (AUP) ..... **Error! Bookmark not defined.**
Acceptable Use of Technology for Staff, Visitors and Volunteers Sample Statements 11
Staff Acceptable Use of Technology Policy (AUP) 11
Staff Acceptable Use of Technology Policy: Key Expectations Summary **Error! Bookmark not defined.**
Visitor/Volunteer Acceptable Use of Technology Policy ..... **Error! Bookmark not defined.**
Wi-Fi Acceptable Use Policy 19
Template Acceptable Use Policy (AUP) for Remote/Online Learning 21
Remote/Online Learning AUP Template - Staff Statements 23
Remote/Online Learning AUP Template – Pupil/Student Statements ..... **Error! Bookmark not defined.**

Child Acceptable Use of Technology Statements

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 check with a grown-up before I click on links or things online.
- 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
- If I see something online that makes me feel upset, unhappy, or worried, I will always tell a grown-up .
- I can visit www.ceopeducation.co.uk to learn more about keeping safe online.
- I know that if I do not follow the school rules:
    - I will not be allowed to use the device and I will need to talk about my behaviour to a headteacher and my parents
- I have read and talked about these rules with my parents.

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 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 I know what they do, or I will ask a safe adult first.
- I will only chat with people I know online, or I will ask a safe adult to help me decide if someone I don't know is safe to speak with online.
- If someone online asks to meet me, I will tell a safe adult straight away.

Learning

- I follow the school rules about mobile phones and smart technology. If I bring a mobile phone or smart device to school I must hand it into the office, I will not use it during the school day, unless a member of staff has agreed this.
- 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.
- If I need to learn online at home, I will follow the same rules in this policy.

True

- I know that some things or people online might not be honest or truthful.
- If I'm unsure if something online is true, I will check other websites, books, or ask a safe adult.
- I always credit the person or source that created any work, images, or text I use.
- I will only use Artificial Intelligence (AI) tools when a safe adult says it is allowed.
- I will not put personal information about me or anyone else into AI tools. I will not use AI to make fake images, voices, videos or messages about other people.

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, upset, or frightened, I will ***shut the laptop lid and tell an adult immediately.***
- If I am aware of anyone being unkind or unsafe with technology, I will report it to a teacher school.
- If an AI tool shows me something worrying, unkind, rude, violent, confusing or unsafe, I will stop and tell a safe adult.
- I understand that the adults at school are responsible for keeping me safe; they may need to speak to other safe adults, or my parents/carers, if I tell them about something that has happened online.
- I can visit www.ceopeducation.co.uk and www.childline.org.uk to learn more about being safe online or to seek help.

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 Teams if they are worried about my or anyone else's safety or behaviour.
- If I bring a mobile phone or other device I will follow the rules. I know that it is to be handed in to the office and then collected at the end of the school . I will not use it during the day unless a member of staff has agreed this
- I understand that my behaviour online can affect others and I will not behave in a way that will upset, frighten or embarrass others.
- I have read and talked about these rules with my parents/carers.
- I know that if I do not follow the school rules then:
    - I may not be allowed to work on computers at school
    - I will be sent to speak to a head teacher
    - My parents will be told

Shortened KS2 version (for use on posters)

- I ask a teacher 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 something which makes me feel worried.
- I know my use of school devices and systems can be monitored.

Children/Pupils/Students with Special Educational Needs and Disabilities (SEND)

Learners with SEND functioning at Levels P4 –P7

- I only use phones, tablets or computers when a grown-up says it is okay.
- I make good choices on the computer.
- I use kind words on the internet.
- I tell a grown-up if I see or hear something online that upsets me.
- I know that if I do not follow the school rules then:
    - I will need to talk to a headteacher and my parents will be told

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

Safe

- I ask a grown up if I want to use a phone, tablet or computer.
- I do not tell strangers my name on the internet.
- I know that if I do not follow the school rules then:
    - I will need to talk to a headteacher and my parents will be told

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 online that worries me, I will tell a grown up.

Learners with SEND functioning at Levels L2-4 (Based on Childnet's SMART Rules)

Safe

- I ask an adult if I want to use the internet.
- I use phones, tablets or computers when an adult says it is okay.
- I keep my information private on the internet.
- I ask an adult before I take or share a photo, video or message.
- I know that if I do not follow the school rules then:
  - I will need to talk to a headteacher and my parents will be told

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 worries or upsets me, I will tell a teacher.

Acceptable Use of Technology Statements and Forms for Parents/Carers

St Katharine's Acceptable Use of Technology Policy Acknowledgement

1. I have received and read St Katharine's Acceptable Use of Technology Policy (AUP) and have discussed its expectations with my child in a way that is appropriate to their age, understanding and needs.

2. I understand that the AUP explains how my child is expected to use technology safely, kindly, lawfully and responsibly, including when using:
    - School-provided devices, accounts, systems and internet access;
    - School-provided technology away from the setting;
    - personal devices or services where their use affects the safety or wellbeing of a child or another person, disrupts the safe or effective operation of the school, or raises a safeguarding or behaviour concern.

3. I understand that access to online content through school devices and systems is appropriately filtered and that use of school-provided devices, accounts and systems may be monitored, including when they are used away from the setting. The school has provided information about its filtering and monitoring arrangements in the Child Protection Policy on its website

4. I understand that filtering and monitoring arrangements help to keep children safe, protect systems and support compliance with relevant policies, but cannot remove every online risk. Monitoring will be proportionate and undertaken in accordance with data protection, privacy and human rights requirements.

5. I am aware of the school's expectations concerning mobile phones and smart devices and will support my child to follow them. If my child may need an exception or reasonable adjustment because of a disability, medical condition, communication need or other individual circumstance, I will discuss this with the school so that appropriate arrangements can be considered, agreed and recorded. I will support any individual arrangements agreed for my child. If I need to contact my child during the school day, I will use the school office or another agreed contact route, unless an alternative arrangement has been agreed.

6. I will support my child to understand and follow the school's expectations for technology use, including social media, mobile phones, online communication, images and recordings and, where relevant, artificial intelligence tools.

7. I will model safe, positive and respectful online behaviour and support my child not to create, post or share content that identifies, targets, threatens, bullies, harasses or risks

causing harm to a child, family, member of staff or another member of the school community.

8. If I have a concern or complaint, I am encouraged to use the school's established communication, safeguarding or complaints routes, as appropriate, so that it can be properly considered.

9. I will report concerns about my child's online safety, or online concerns that may affect the safety or wellbeing of another member of the school community, to an appropriate member of staff. This may include class teacher, the Designated Safeguarding Lead or headteacher. Where necessary, I may also report the concern to another relevant organisation.

10. If the school has concerns about my child's online safety or behaviour, I understand that these will be considered fairly and proportionately in line with relevant safeguarding, behaviour and other procedures. The school will communicate with me where it is appropriate and safe to do so.

11. I understand my role in helping my child to use technology safely. As appropriate to my child's age, understanding and needs, I will consider the use of parental controls, provide suitable supervision and support, and encourage safe and responsible use of the internet and other technology at home.

12. I know that I can seek online safety information or support from the school by following links on the school website or coming to the office.

I acknowledge that I have received and read the St Katharine's Child Acceptable Use of Technology Policy and have discussed its expectations with my child.

Child's name: .....

Class/group: .....

Child's signature: ..... ***(if appropriate)***

Parent/carer's name: .....

Parent/carer's signature: .....

Date: .....

Acceptable Use of Technology for Staff, Visitors and Volunteers Statements

Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all staff are expected to use technology in a professional, lawful, ethical and responsible manner.

This Staff Acceptable Use of Technology Policy (AUP) sets out St Katharine's, expectations for safe technology use, professional conduct, safeguarding, data protection and system security. It is not intended to unduly limit appropriate teaching, learning or professional use of technology, but to help protect children, staff, systems and the wider school community from accidental or deliberate misuse.

All staff are asked to read, understand and sign this AUP.

Policy scope

I understand that this policy applies to my use of technology systems and services provided by the school or accessed by me as part of my role within St Katharine's both on and offsite. It also applies to personal use of technology where this is linked to my role, involves the school community, uses school systems or information, could affect safeguarding, professional boundaries, confidentiality or data protection, or could reasonably impact on my professional role or the reputation of the school.

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

I am aware that all staff should ensure that technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of St Katharine's devices and systems

I will use school provided or approved equipment, systems and internet services when working with children, unless otherwise formally agreed by leaders.

I understand that school equipment, systems and internet services are provided for education and/or professional use.

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

Data and system security

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 follow the school's requirements for secure passwords, authentication and account access. I will keep authentication information secure and will not share passwords, verification codes or access credentials with others.
- I will protect the devices in my care from unapproved access or theft.

I will take care before opening links or attachments, including those apparently sent by a known contact. I will check unexpected or suspicious messages through an appropriate route and report suspected phishing or malicious content to the office

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

I will ensure that any personal data is kept in accordance with data protection legislation, 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
- I will only process or share personal data through school -approved systems and services and in line with the setting's data protection and information-security procedures. Any proposed new or changed use of cloud services, AI tools or other online systems involving personal data will be risk assessed and approved through the setting's agreed process before use. Where required, a Data Protection Impact Assessment will be completed.

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 VPN.

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

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.

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

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

If I have lost any school related documents or files, I will report this to the office and school Data Protection Officer (Sarah Jane Tormey) as soon as possible.

I will follow the image use policy when taking, using, storing or sharing images or recordings of children Images and recordings must always be appropriate and must only be taken using school-provided or approved equipment. I will not use personal devices, including personal mobile phones, cameras, tablets, smart watches or other wearable technology, to take images or recordings of children. Images and recordings will only be taken, used or shared in line with the image use policy, safeguarding expectations, data protection requirements and consent/lawful basis arrangements.

Classroom practice

I understand my role and responsibilities in relation to filtering and monitoring, as explained through induction, safeguarding training and relevant policies.

If I become aware of a filtering or monitoring failure, or witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT provider/staff, in line with the child protection policy.

I will follow school expectations for safe technology use in classrooms, remote/online learning and other working spaces, including the use of approved platforms, search tools and AI tools.

I will follow the setting's agreed approach to screen use. Any use of screens, devices, apps or online content will be planned, purposeful, age appropriate and supervised, and will not replace face-to-face interaction, play, physical activity, rest, care routines or real-world exploration.

2. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I 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, their use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that:
    - AI tools must only be used responsibly, ethically and where the tool, purpose and use have been approved by leaders. Any new, unapproved or changed use of AI tools will be risk assessed and approved before use, in line with child protection, data protection and professional conduct expectations.
    - I understand that AI-generated content must be checked for accuracy, bias, appropriateness, copyright and safeguarding implications before it is used or shared.
    - I will not enter personal, sensitive, confidential, safeguarding, assessment or special category information, or images of children, staff or other identifiable individuals, into any AI tool unless the tool has been approved for that purpose, the use has been risk

assessed, consent has been obtained where required, and the leadership teamhas confirmed that the processing is lawful and appropriate.

- I will not add or use AI note takers, transcription tools, recording bots or automated meeting summary tools in any meeting, lesson, supervision, training or professional discussion unless this has been agreed in advance by leadership. Where approved, I will ensure that participants are made aware and their use is transparent, proportionate and in line with safeguarding, confidentiality, consent, data protection and information governance expectations.
- I will not use AI to make decisions about children, families or staff, including decisions relating to safeguarding, behaviour, SEND, assessment, attendance, admissions, recruitment, allegations or pastoral support, without appropriate professional oversight and in line with setting policy.
- 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.
- I will report any concern involving AI misuse, including deepfake or manipulated content, impersonation, harmful AI-generated material, AI-facilitated bullying or harassment, or AI-generated nude/semi-nude imagery, in line with the school child protection, behaviour, anti-bullying, staff conduct and data protection procedures

3. 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 or being judged for talking about something which happened to them online.
    - involving the DSL or a deputy 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.
    - making informed decisions to ensure any online safety resources used with children are appropriate.

4. 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 phones and smart devices

.

5. I will ensure that my use of mobile phones and smart devices is compatible with my professional role, does not interfere with my duties, and takes place in line with the staff behaviour policy/code of conduct, mobile phone policy and the law.

6. I will model safe and professional use of mobile phones and smart devices and will support the school ’s expectations for children

7. Where mobile phones or smart devices are used for professional purposes, such as authentication I will ensure this is done promptly and my phone then put away.

8. Any use of a personal mobile phone or smart device for professional purposes, or in exceptional circumstances, must be transparent, necessary, proportionate and approved by the headteacher. Use must not compromise supervision, safeguarding, confidentiality, professional boundaries, data protection or the learning environment.

Online communication, including use of social media

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

10. I will protect myself, my professional reputation and the reputation of the St Katharine’s online. I will not discuss or share data or information relating to children, staff, school business or parents/carers on social media.

11. My electronic communications with current and former 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-provided communication channels and systems, such as a school email address, user account or telephone number.
    - I will not use personal accounts, personal profiles, personal phone numbers, private messaging apps, gaming accounts or other personal communication channels to contact or communicate with children or their families, unless this has been formally approved, risk assessed and recorded by leaders.
    - I will not share any personal contact information or details with children, such as my personal address, email address or phone number.
    - I will not share personal information about my private life with children. online, through messaging, social media, gaming platforms, apps or other digital communication channels. I will maintain appropriate professional boundaries in all digital communication.

- I will not add, follow, accept or respond to friend requests, direct messages or other personal online communication from current or former children, or their parents/carers, where this is linked to my role, the school or could blur professional boundaries. Any attempted contact will be reported to my line manager and/or the DSL.
- Any pre-existing links, relationships or situations that affect how I apply the AUP or other relevant policies will be discussed with the DSL and/or headteacher. This is to help safeguard children, staff and the wider school community by ensuring professional boundaries, safeguarding expectations and communication arrangements are clear. **.**
- Where digital communication with children or families is required, I will follow the school expectations about when communication should take place, including any agreed arrangements for out-of-hours contact, emergency communication or role-specific responsibilities. ***The headteacher email is monitored out of hours and staff will respond to emails within 48 hours.***

Policy concerns

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

13. I will not access, create, transmit, display, publish, forward, discuss, send, share or show any material or content that may be harmful, inappropriate, adult, offensive, unprofessional, or likely to harass, cause offence, inconvenience or needless anxiety to any other person. This applies when using school systems, school devices, personal devices, personal accounts, messaging apps, online platforms, social media or shared spaces. It includes content shared in staff rooms, offices, online groups or other staff communication spaces, where this takes place on school premises, during working time, or in any context linked to my role.

14. I will not engage in online or digital behaviour linked to my role that compromises safeguarding, professional boundaries, confidentiality, data protection, public confidence in my professional conduct or my ability to carry out my role.

15. 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 child protection policy.

16. I will report concerns about the welfare, safety, conduct, or behaviour of staff, including online, digital, device-related or technology-linked concerns, to the headteacher], in line with the school child protection policy, staff behaviour policy/code of conduct, low-level concerns procedures and/or allegations against staff policy.

Policy compliance and breaches

17. 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 DSL and the headteachers .

18. I understand that the school may exercise its right to monitor the use of its devices and information systems to check policy compliance and help ensure the safety of children and staff.

- This includes monitoring all school-provided devices and school/setting 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.

- Staff will be informed about the nature, purpose and extent of monitoring through this AUP, relevant policies, privacy information and/or staff guidance.

19. I understand that if the school believes 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

20. If I find myself in a situation where my online contact, device use, recording, image use or AI use could be misinterpreted, I will report this promptly to the DSL/headteachers so it can be recorded and managed transparently.

21. Any breach or concern involving online contact, device use, images, recordings, social media, AI use, confidentiality, data protection or professional boundaries must be reported to the headteachers/DSLs without delay, even if it appears minor, accidental or unlikely to meet the harm threshold.

I understand that if the school believes that unprofessional or inappropriate online or technology-related activity may have compromised safeguarding, professional boundaries, confidentiality, data protection, public confidence in professional conduct or my ability to carry out my role, the concern will be considered fairly, proportionately and confidentially, in line with relevant safeguarding, staff behaviour, low-level concerns, allegations, data protection and disciplinary procedures. Where the concern may meet the harm threshold, advice will be sought and/or a referral made to the Local Authority Designated Officer (LADO) in line with local allegations procedures. Where it does not meet this threshold, it will still be recorded and responded to appropriately.

22. Where a concern involves personal data, confidential information, safeguarding information, images, recordings, AI tools, transcription tools or unauthorised sharing, the DPO/data protection lead will be informed promptly so that any data protection, information governance or reporting requirements can be considered.

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

24. I understand that this AUP cannot cover every possible situation. If I am unsure whether any use of technology, online communication, image use, recording, personal device use, social media, AI tool or digital contact is appropriate, I will seek advice from the DSLs/headteachersr] before taking action. I will act in a way that safeguards children, protects professional boundaries, and is open to scrutiny.

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

Name: ……

Signed: …….....

Date (DDMMYY):……...

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for safeguarding children, all users must understand the boundaries and expectations when using the school Wi-Fi. Users are expected to use Wi-Fi safely, lawfully and responsibly, and to take reasonable steps to protect devices, data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list. All users are reminded that technology use should be consistent with the school ethos, relevant policies and the law.

1. The school setting provides Wi-Fi for education use only.

2. Use of the Wi-Fi falls under St Katharines Acceptable Use of Technology Policy (AUP), the child protection policy, behaviour policy/code of conduct, data protection/security policies and any other relevant policies. All children, staff, visitors and volunteers using the Wi-Fi must comply with these expectations.

3. The school reserves the right to limit, restrict, withdraw or manage Wi-Fi access where necessary to maintain safeguarding, security, network reliability or fair use of network resources.

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

5. I will take reasonable steps to ensure that any personal device connected to school Wi-Fi is appropriately secure, for example by using security updates, antivirus protection where appropriate, and secure passwords/PINs.

6. I will respect system security and will not share passwords, Wi-Fi access details or security information. I will not attempt to bypass security, filtering or monitoring systems, or download unauthorised software, applications or files.

7. I will not use school Wi-Fi to access, create or share illegal or harmful content, compromise another person’s safety or privacy, interfere with systems, or breach relevant school policies.

8. I will not use school Wi-Fi to access, store, send or share confidential, personal or safeguarding information unless this has been specifically authorised and is in line with school data protection and safeguarding procedures.

9. Staff using school Wi-Fi on personal devices remain subject to the staff behaviour policy/code of conduct, Staff AUP, mobile phone/smart device policy, data protection expectations, and relevant safeguarding and disciplinary procedures.

10. The school takes reasonable and proportionate steps to manage the security of its Wi-Fi service. However, no wireless or internet service can be guaranteed to be free from all risk. Where personal devices are permitted to connect to the school Wi-Fi, users do so at their own discretion and are expected to keep their devices secure. Any concerns about Wi-Fi security, filtering, monitoring or device safety should be reported to the DSL or identified technical contact.

11. I will report any online safety concerns, filtering breaches, security concerns, or access to inappropriate materials to the Designated Safeguarding Leads [Sarah Jane Tormey and Xanthe Veneziani] or identified technical contact as soon as possible. If I have any queries about safe behaviour online, I will speak to the DSL, identified technical contact or headteacher

12. I understand that activity carried out through school Wi-Fi may be monitored and recorded to check policy compliance, protect systems and help keep users safe, including where the Wi-Fi is accessed using a personal device. This does not mean that the school can monitor other activity or information held on the personal device. Monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

13. If the school suspects that unauthorised or inappropriate use, unacceptable behaviour, a data protection concern, a safeguarding concern or criminal activity may have taken place, access may be restricted or withdrawn and the concern may be managed in line with relevant [school/setting] procedures. Where appropriate, this may include informing the DSL, Data Protection Officer, headteacher/manager, employer/organisation, LADO or police.

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 address safer practice when using remote/online learning, live-streamed sessions, video conferencing, online tutoring, remote meetings and other online communication involving children/pupils/students and families. Settings should implement the approaches that best suit the needs of their community following appropriate safeguarding, technical and data protection consideration.

Remote/online learning or communication should only take place using setting-approved systems, accounts and devices wherever possible. Leaders should ensure any platform used has been appropriately assessed, including consideration of safeguarding, privacy, data protection, age restrictions, recording, chat, screen-sharing, access controls, retention and reporting arrangements

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:

- 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 Knockholt Staff Remote/Online Learning AUP

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

Leadership oversight and approval

1. Remote/online learning will only take place using Teams.
    - Teams has been assessed and approved by Sarah Jane Tormey.

2. Staff will only use school managed, approved professional accounts with children and 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 the Designated Safeguarding Leads(DSLs).
    - Staff will use work provided equipment where possible. ***If this is not provided, leaders should ensure clear expectations are in place in relation to safeguarding and data security when using personal devices, eg using strong passwords, suitable levels of encryption, logging off or locking devices when not in use etc.***

3. Online contact with children and parents/carers will not take place outside of the operating times as defined by SLT:
    - 9am to 3.30pm.

4. All remote/online lessons will be formally timetabled**;** a member of SLT will be able to drop in at any time.

5. Live-streamed remote/online learning sessions will only be held with approval and agreement from the headteachers.

Data Protection and Security

6. Any personal data used by staff and captured by Teams when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy

7. All remote/online learning and any other online communication will take place in line with current confidentiality expectations as outlined in Confidentiality policy.

8. 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.
9. Only members of the school community will be given access to Teams

10. AI note takers, transcription tools, recording bots or automated meeting summaries must not be used in remote/online learning, meetings or training unless this has been approved in advance by leaders and is managed in line with safeguarding, consent, confidentiality and data protection requirements.

Session management

11. Staff will record the length, time, date, and attendance of any sessions held.

12. Appropriate privacy and safety settings will be used to manage access and interactions.

13. Live sessions will follow the school's agreed staffing, oversight and audit arrangements:

14. Live 1:1 sessions will only take place with approval from the headteacher. ***Any one-to-one remote session must be necessary, authorised and conducted in line with the setting's child protection, staff behaviour and safer working practice arrangements. Leaders should define appropriate oversight, transparency, communication with parents/carers where appropriate, record keeping, auditability and arrangements for safeguarding or therapeutic confidentiality.***

15. A pre-agreed invitation detailing the session expectations will be sent to those invited to attend.
    - Access links should not be made public or shared by participants.
    - Children and parents/carers should not forward or share access links.
    - Staff will explain any expectations about the location from which children take part. These will reflect their age, needs, privacy, home circumstances and the nature of the session.

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

Behaviour expectations

17. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.

18. All participants are expected to behave in line with existing school policies and expectations. This includes:

- ***Appropriate language will be used by all attendees.***
- ***Appropriate clothing to be worn***
- ***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.***

19. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.

20. When sharing videos and/or live streaming, participants are required to:
    - ***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.***

21. 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

22. **Participants are encouraged to report concerns during remote and live-streamed sessions:**
    - **Telling a trusted adult**

23. **If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to the headteachers**

24. **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.**

25. **Sanctions for deliberate misuse may include *: restricting/removing use, seeking police or other appropriate advice where behaviour may be unlawful or presents a risk to safety***

26. **Any safeguarding concerns will be reported to Sarah Jane Tormey or Xanthe Veneziani , Designated Safeguarding Leads, 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: ……

27.

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, Ifield 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.