



**Canterbury Road Primary School**

# **Acceptable Use of Technology Policy**



Written/adopted: **December 2023**

To be reviewed: **September 2024**

By: **Mr Pye (DSL)**

# Contents

Contents.....	2
Early Years and Key Stage 1 (0-6).....	3
Key Stage 2 (7-11) .....	3
Acceptable Use of Technology Sample Statements and Forms for Parents/Carers .....	7
Parent/Carer AUP Acknowledgement Form.....	7
Visitor and Volunteer Acceptable Use of Technology Policy .....	12
Wi-Fi Acceptable Use Policy.....	15
Template Acceptable Use Policy (AUP) for Remote/Online Learning .....	17
Acknowledgements and Thanks .....	17

# Pupil - Acceptable Use of Technology

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

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

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

- I understand that the school Acceptable Use Policy will help keep me safe and happy online.
- I only use the internet when an adult is with me.
- I only click on online links and buttons when I know what they do. If I am not sure, I ask an adult first.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online when I use school computers and tablets, including if I use them at home.
- I always tell an adult if something online makes me feel upset, unhappy, or worried.
- I can visit [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) to learn more about keeping safe online.
- I know that if I do not follow the school rules:
  - **Golden Time will be taken away**
  - My parents will be called
  - I may be excluded
- 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 behave online the same way as I behave in the classroom.

- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are safe and appropriate, and if I have permission.
- I only talk with, and open messages, from people I know.
- I will only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.
- I will not arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- If I get unpleasant, rude, or bullying emails or messages, I will report them to a [teacher](#) or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.

## Learning

- I ask my teacher before using my own personal smart devices and/or mobile phone at school. If I bring my device to school I will give it to a class teacher to be locked away or in the school office.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use school/ devices for school work unless I have permission otherwise.
- If I need to learn online at home, I will follow the school remote/online learning AUP and only access websites my teacher has chosen.

## Trust

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

## Responsible

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

## Tell

- If I see anything online that I should not or if I see something online that makes me feel worried or upset, I will minimise the screen and tell an adult immediately.
- If I am aware of anyone being unsafe with technology, I will report it to adult at school.
- I know it is not my fault if I see, or someone sends me, something upsetting or unkind online.
- I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.

## Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all Canterbury Road owned devices and networks are monitored to help keep me safe, including 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 networks if they are concerned about my or anyone else's safety or behaviour.
- If, for any reason, I need to bring a personal device, for example a smart/mobile phone and/or other wearable technology into school then I will make sure I tell the class teacher and put it in the classroom cupboard or hand it in to the school office.
- I have read and talked about these rules with my parents/carers.
- I can visit [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) and [www.childline.org.uk](http://www.childline.org.uk) to learn more about being safe online or to see help
- I know that if I do not follow the school rules then:
  - I can have the devices taken away
  - I can lose Golden Time
  - I can have my parents called or face exclusion

## 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.

# Pupil/Student Acceptable Use Policy Agreement Form

## Canterbury Road Acceptable Use of Technology Policy – Pupil Agreement

I, with my parents/carers, have read and understood the school Acceptable Use of Technology Policy (AUP)

I agree to follow the AUP when:

1. I use school devices and systems, both on site and at home.
2. I use my own equipment out of the school, including communicating with other members of the school or when accessing school systems..

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

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

Parent/Carer's Name.....

Parent/Carer's Signature.....

Date.....

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

## Parent/Carer AUP Acknowledgement Form

### Canterbury Road Primary School Pupil Acceptable Use of Technology Policy Acknowledgment

1. I have read and discussed Canterbury Road Primary School 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 including laptops, ipads, tablets and phones and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another pupil, could have repercussions for the orderly running of the school, if a pupil is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.
3. I understand that any use of school devices and systems are appropriately filtered; this means that EIS Smoothwall follow can restrict and monitor access to apps, websites and pages and social media.
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. This includes the head teacher receiving a report of anything accessed or searched for that may be inappropriate. This is currently operated by EIS and Smoothwall. 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.
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.
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 schools 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.....

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

Parent/Carer's Name.....

Parent/Carer's Signature.....

Date.....



## Classroom practice

1. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by Canterbury Road as detailed Acceptable Use Policy and Child Protection Policy, and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.
2. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT provider, in line with the school/ child protection/online safety policy.
3. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in, child protection, online safety, remote learning AUP Policy.
4. 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) (T Pye, K Martin, S Brown, Debbie Gallier) 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.
5. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

## Mobile devices and smart technology

6. I have read and understood the school mobile and smart technology and social media policies which addresses use by children and staff.
7. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff code of conduct and the school mobile technology policy and the law.

## Online communication, including use of social media

8. I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the child protection policy, staff code of conduct, social media policy and the law.
9. As outlined in the staff code of conduct and school 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.
10. 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 Designated Safeguarding Lead (DSL).
  - Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL and/or headteacher/manager.

## Policy concerns

11. 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.
12. 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.
13. 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.
14. 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.
15. 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

16. 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.
17. 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.
18. I understand that if the school believe that unauthorised and/or inappropriate use of school devices, systems or networks is taking place, the school may invoke its disciplinary procedures as outlined in the staff code of conduct.
19. 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 code of conduct.
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 Canterbury Road 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 Canterbury Road Primary 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 Canterbury Road Primary, 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 Canterbury Road Primary School AUP should be read and followed in line with the school staff 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 will ensure that any access to personal data is kept in accordance with Data Protection legislation, including UK GDPR.
8. I understand that I am not allowed to take images or videos of children without prior consent. Any images or videos of children will only be taken in line with the school camera and image use policy.

## **Classroom practice**

9. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of children.
10. Where I deliver or support remote/online learning, I will comply with the school remote/online learning AUP.
11. 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.
12. 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 provider EIS in line with the school child protection policy.
13. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music is protected, I will not copy, share, or distribute or use it.

## **Use of mobile devices and smart technology**

14. In line with the school mobile and smart technology policy, I understand that, mobile phones and personal devices are not permitted or are only permitted within specific areas.
15. In an emergency permission from the DSL should be gained before taking my phone into an area with children.

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

16. 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 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 code of conduct and the law.
17. 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 (T Pye).

## Policy compliance, breaches or concerns

18. 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 (T Pye)
19. 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.
20. I will report and record concerns about the welfare, safety or behaviour of children or parents/carers online to the Designated Safeguarding Lead (T Pye) in line with the school child protection policy.
21. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with the allegations against staff policy.
22. 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.
23. 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 Canterbury Road Primary 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 education use 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 Canterbury Road Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy Child Protection Policy, 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 (T Pye) as soon as possible.
14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (T Pye).
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 Canterbury Road Wi-Fi Acceptable Use Policy.**

Name .....

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



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

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

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

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

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

## Acknowledgements and Thanks

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

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