



Claremont Primary School

A hub of educational excellence and innovation,
supporting and valuing everyone

Acceptable Use of Technology Policy

Responsible person	Clare Smith, Designated Safeguarding Lead
Responsible governor	Rob Jackson, Safeguarding Governor
Responsible governor team	FGB
Date approved	Autumn 2026
Date of next review	Autumn 2027
Policy reference	Adopted KCC/The Education People

At Claremont we believe and recognise that the diversity of our community is one of our greatest strengths and assets. We are committed to ensuring that our pupils are treated fairly, and we have carefully considered and analysed the impact within this policy to promote equality of opportunity for all and we will use our position of influence as a school to work with all stakeholders to eliminate discriminatory barriers and ensure that our pupils have a sense of shared, common belonging and understanding

1. Policy Aims

1.1 At Claremont Primary School, we want to ensure that all members of our community are safe and responsible users of technology. We will support our pupils to:

- Become empowered and responsible digital creators and users
- Use our resources and technology safely, carefully and responsibly
- Be kind online and help us to create a community that is respectful and caring, on and offline
- Be safe and sensible online and always know that you can talk to a trusted adult if you need help

2. Policy Structure

This policy is in the form of adapted Acceptable Use Policy which each member of our school community will be expected to abide by. They are in a format that is relevant and accessible, and are adapted to ages/roles of each group in the school.

3. Claremont Primary School's Responsibilities

3.1 This Policy is designed with the aim of keeping our school and its members, both child and adult, safe from online and technological threats and encourage safe and responsible use of technology.

3.2 We understand that we have an important role to play and we agree that we will:

- Keep our technology (hardware and software) as up to date as we are able to
- Maintain an efficient, effective and up-to-date filtering and blocking system on our internet connection
- Monitor the use of our systems (in accordance with legislation)
- Provide age-appropriate, up-to-date online safety education for our pupils
- Encourage responsible and safe use of technology resources
- Provide appropriate supervision for pupils using technology
- Act on any reports of online safety incidents or breaches of the Acceptable Use Policy
- Enforce fairly and appropriately the terms of the AUPs and agreements throughout school.

4. Pupils' Policies

4.1 Pupils in Early Years and Key Stage 1

4.1.1 Parents/Carers of will be sent the Pupils and Parents/Carers Acceptable Use of Technology documents (detailed below). They are asked to read and explain the content of the Policy to their child and then sign and return the agreement form on their behalf. The form will be signed by parents annually.

4.2 Pupils in Key Stage 2

4.2.1 As with pupils in Key Stage 1, Parents/Carers will be asked to read, explain (when necessary) and discuss the policy with the child. Because the children are now old enough to understand, the child will be expected to sign the agreement as well as the parent/carer, saying that the child understands and that they agree to abide by the Policy. This will be completed annually.

5. Staff Policy

5.1 As a professional organisation with responsibility for safeguarding, Claremont School believes it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's IT systems in a professional, lawful, and ethical manner.

5.2 To ensure that members of staff are fully aware of their professional responsibilities when using technology, they will be expected to read and sign the Staff Acceptable Use Policy agreement when they join the school, and when it is updated each year. A copy of the signed agreement will be kept on file. Failure to abide by the Staff Acceptable Use Policy agreement may result in disciplinary action being taken.

5.3 Staff are reminded that under the terms of the school Child Protection and Safeguarding Policy, they should not use personal devices during teaching periods, unless permission has been given by the Headteacher, such as in emergency circumstances.

5.4 Staff should use the school WiFi on their personal devices while on the premises. Paragraphs about the use of the WiFi network are included in the Staff Acceptable Use Policy. Staff are reminded that usage is monitored and that the network is filtered and limits or prevents access to certain websites.

6. Visitors, Volunteers and Contractors

6.1 As a professional organisation with responsibility for safeguarding, Claremont School believes it is important that visitors, volunteers and contractors understand the risks involved with the use of mobile phones and devices on the school site, and the needs to place strict limits on that use.

6.2 Most mobile phones and devices now include a camera facility, and this allows photographs to be taken with ease in any location. Mobile data allows the easy transfer of images from device to device, and users can receive (willingly or not) inappropriate images on their mobile devices. Claremont School has a duty to protect the pupils under its care and therefore needs to reduce the risk of unauthorised images being obtained of children in school, and/or of children being exposed to inappropriate images, even accidentally.

6.3 In order to reduce these risks, Claremont Primary School asks **that visitors avoid all use of personal mobile devices while they are on the school property.**

If it is absolutely necessary for that device to be used, eg. caretaker, contractor, it must be used in an area where no pupils are present and a member of the SLT advised.

6.4 Our procedures to deal with this are as follows:

- 1) Visitors to the site who sign in are all asked to confirm by ticking in the visitors' book that they have read the Safeguarding for Visitors green leaflet. This includes regular contractors to the school, who are DBS checked and vetted by KCC.
- 2) Volunteers who may spend longer periods unaccompanied by staff while in school will be asked to sign an Acceptable Use Agreement formally agreeing to this usage limitation.
- 3) Contractors who will be working on site for extended periods in term time will be asked to agree to this usage limitation as part of the pre-commencement procedures and agreements.

Pupil Acceptable Use of Technology

Early Years and Key Stage 1

- I understand that the school's rules will help keep me safe and happy when I go online.
- I only go online when an adult is with me
- I check with an adult 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 a school computer and iPads
- I use the iPads for what I have been asked and I use my allocated iPad
- If I see something online that makes me feel upset, unhappy or worries, I will always tell an adult.
- I can visit www.thinkuknow.co.uk, CEOP Education and www.childline.org.uk to learn more about being safe online.
- I know that if I do not follow the rules, my teacher might give me a yellow or red card. They might also talk to my parents.
- I have read and talked about these rules with my parents/carers

Key Stage 2

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 at 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 trusted 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 'brick' phone to school, I will not use it during the school day.
- 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 the iPads for what I have been asked and I use my allocated iPad
- I use school computers for school work, unless I have permission otherwise

True

- I know that some things or people online might not be honest or truthful
- If I'm unsure something online is true, I will check with other websites, books or ask a trusted adult.
- I will always credit the person or source that created any work, image or text I use.
- I will only use Artificial Intelligence (AI) tools when a trusted 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 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 report it to a teacher or other adult.
- If I am aware of anyone being unkind or unsafe with technology, I will report it to a teacher or other adult.
- 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.thinkuknow.co.uk, 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. This means someone at the school may be able to see and check my online activity when I use a school device or network if they are worried about my or anyone else's safety or behaviour.
- If I am in Year 6 and bring my 'brick' phone to school, I will hand it in at the beginning of the day to the adults in my class. I will keep it turned off when I am in school, unless an adult has given me permission to turn it on.
- I know that if I do not follow the rules, my teacher might give me a red card. They will also talk to my parents.
- 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

Claremont Acceptable Use of Technology Policy
Pupil Agreement

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

I agree to follow the AUP when:

1. I use Claremont-approved systems and devices, both on and offsite.
2. I use my own equipment outside school, in a way that is related to me being a member of the Claremont community, including communicating with other members of the school.

Name

Signed

Class Date

Pupils in KS2 should sign this agreement themselves; parents of children in KS1 may sign it on their behalf once the information has been discussed.

Parent/Carer Acceptable Use of Technology Policy (AUP)

1. Access to technology

I understand that my child will be provided with internet access and may use a range of technology, devices, accounts and online services at Claremont Primary School including computers, iPads and laptops to support their learning, development and preparation for life in a digital world.

2. Scope of the Pupil AUP

I understand that the Pupil AUP applies to my child's use of school-provided devices, accounts, systems and internet access, both on site and when accessed away from the school.

Relevant school expectations may also apply to personal technology use where online behaviour:

- affects the safety or wellbeing of a child, member of staff or another person;
- disrupts the safe or effective operation of the school; or
- raises a safeguarding, behaviour or potentially unlawful concern.

3. Understanding the Pupil AUP

I have received and read Claremont Primary School's Pupil Acceptable Use of Technology Policy and have discussed its expectations with my child in a way that is appropriate to their age, understanding and needs.

4. Supporting safe and responsible technology use

I will support my child to understand and follow the school's expectations for safe, kind, lawful and responsible use of technology. This includes expectations relating to online communication, social media, images and recordings and, where relevant, artificial intelligence tools.

I understand that guidance, legislation, technology and online risks may change and that the school may review and update its policies and expectations in response.

5. Mobile phones and smart technology

I am aware that the school has clear expectations concerning children's use of mobile phones and smart technology.

In schools, pupils should not bring in, use, access, display or check mobile phones or similar smart technology during the school day, including during lessons, time between lessons, breaktimes and lunchtime, unless a specific exception or reasonable adjustment has been agreed.

Where my child may need access to a mobile phone or smart device because of a disability, medical condition, communication need or other individual circumstance, I will discuss this with the school. Any exception or reasonable adjustment will be considered individually and, where agreed, the purpose, arrangements and expectations for use will be clearly recorded and communicated to my child and relevant staff.

I will support the school's expectations and any individual arrangements agreed for my child. I will not contact my child directly on their mobile phone or smart device during the school day unless this forms part of an agreed arrangement. If I need to contact my child during the day, I will use the school office or another agreed contact route.

6. Filtering

I understand that access to online content through school-provided devices, systems and internet services is appropriately filtered. Information about the filtering arrangements in place is available on our website.

7. Monitoring

I am aware that my child's use of school-provided devices, accounts and systems may be monitored, including when those devices, accounts or systems are used away from the school. Information about the monitoring arrangements in place is available on our website and in our Child Protection Policy.

Monitoring is used to help keep children safe, protect systems and check compliance with relevant policies. It will be proportionate and undertaken in accordance with data protection, privacy and human rights requirements.

8. Limitations of filtering and monitoring

I understand that the school will take reasonable and proportionate steps, including the use of appropriate filtering and monitoring arrangements, to help keep children safe when using school-provided devices and systems.

I understand that no filtering or monitoring system can remove every online risk, particularly where online content changes rapidly or where children use personal devices, accounts, networks or services outside the school's systems.

9. Online safety education

I understand that my child will receive age and ability-appropriate online safety education to help them use technology safely and responsibly, both within and outside the school.

I recognise that education, appropriate supervision, open communication and opportunities to seek help remain important alongside technical measures such as filtering and monitoring.

10. Supporting my child at home

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 suitable parental controls and safety settings;
- provide appropriate supervision, support and guidance;
- talk to my child about their online experiences;
- encourage safe, kind, lawful and responsible online behaviour; and
- help my child understand how and where to seek support.

11. Remote and online learning

Where my child accesses remote or online learning, I will support them to follow the school's remote/online learning expectations. I will help my child to access learning from an appropriate location and provide supervision and support that reflects their age, understanding and needs.

I understand that the school will provide information about the systems and sites my child is expected to access and who from the school, if anyone, they will interact with online.

12. Positive and respectful online behaviour

I will support the school's approach to online safety and model safe, positive and respectful online behaviour, including when creating or sharing images, text, audio or video.

I will 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.

13. Raising concerns and complaints

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 the matter can be properly understood and considered.

Information about how to raise a concern, safeguarding report or complaint is available through the Complaints Procedure on our website.

14. Reporting online safety concerns

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 by email to DSL@claremont.kent.sch.uk or
- the headteacher.

Where necessary, I may also report the concern to another relevant organisation or emergency service.

15. Responding to online concerns

If the school has concerns about my child's online safety, online behaviour or use of technology, I understand that these will be considered fairly and proportionately under the setting's child protection, behaviour and other relevant policies.

The school may also need to consider an appropriate response where online behaviour involving a parent/carer affects the safety or wellbeing of a child, member of staff or another person; disrupts the safe or effective operation of the school; involves

confidential or personal information; or raises a safeguarding or potentially unlawful concern. Any such concern will be considered fairly and proportionately, taking account of the particular circumstances and in line with the school's Complaints Procedure, Parent Code of Conduct, Home-School Agreement or other relevant arrangements.

The school will communicate with those involved where it is appropriate and safe to do so. I understand that there may be circumstances in which the setting must first follow its safeguarding procedures or seek advice from another agency. Where behaviour may be unlawful or presents a risk to safety, the school may seek appropriate safeguarding, police or legal advice.

16. Online safety advice and support

I know that I can seek information or support from the school about online safety and helping my child to use technology safely. Information is available through our website.

17. Agreement

I confirm that I have read and understood the Claremont Primary School Parent/Carer Acceptable Use of Technology Policy and agree to support its expectations and the safe, lawful and responsible use of technology by my child.

Child's Name.....

Child's Signature (if in *in KS2*)

Class Date

Parents Name

Parent/Carer Signature (1)

Date

Parent/Carer Signature (2)

Date

Staff Acceptable Use of Technology

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

This Staff Acceptable Use of Technology Policy (AUP) sets out Claremont Primary School'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 pupils, 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

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed by me as part of my role within Claremont Primary School both on and off site. 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.
2. I understand that Claremont Primary School's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school's Child Protection Policy and the Staff Code of Conduct.
3. 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 School Devices and Systems

4. I will use school-provided or approved equipment, systems and internet services when working with pupils, unless otherwise formally agreed by leaders.
5. I understand that school equipment, systems and internet services are provided for education and/or professional use. Reasonable personal use is permitted during break and lunchtimes away from children and must not interfere with my work duties, system security, safeguarding, confidentiality or professional boundaries. This permission is at the school's discretion and may be withdrawn at any time.
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.
8. 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.
9. I will protect the devices in my care from unapproved access or theft by ensuring they are not left visible or unsupervised in public places.

10. 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 our School Data Protection Officer (Satswana) and/or our ICT Support Provider (Paul Ashmore).
11. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.
12. I will ensure that any personal data is kept in accordance with the 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 hard drives will be suitably protected. This may include data being encrypted by a methods 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 school's agreed process before use. Where required, a Data Protection Impact Assessment will be completed.
13. 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. However, I may access the school email via my mobile phone outside school. An exception may be made for accessing digital learning platforms, with the Headteacher's permission. Where possible, I will use the school learning platform to upload any work documents and files in a password protected environment or school-provided VPN.
14. 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.
15. 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.
16. I will not attempt to bypass any filtering and/or security systems put in place by the school.
17. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Support Provider (Paul Ashmore) as soon as possible.
18. If I have lost any school related documents or files, I will report this to the ICT Support Provider (Paul Ashmore) and School Data Protection Officer (Satswana) as soon as possible.
19. I will follow the school image use policy when taking, using, storing or sharing images or recordings of pupils. 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 pupils. Images and recordings will only be taken, used or shared in line with the school Image Use Policy, safeguarding expectations, data protection requirements and consent/lawful basis arrangements.

Classroom Practice

20. I understand my role and responsibilities in relation to filtering and monitoring, as explained through induction, safeguarding training and relevant school policies.
21. 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 school Child Protection Policy.
22. 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.
23. I will follow the school'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.
24. 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 pupils, 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 DPO has 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 the SLT. 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 pupils, 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 pupils. Pupils 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, Positive Behaviour, Anti-bullying, Staff Code of Conduct and Data Protection procedures.
25. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
- exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
 - creating a safe environment where pupils 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 pupils who may be impacted by the content.
 - informing the DDSL 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 pupils are appropriate.
26. 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

27. 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 Code of Conduct, Mobile & Smart Phone Technology Policy and the law.
28. I will model safe and professional use of mobile phones and smart devices and will support the school's expectations for pupils.
29. Where mobile phones or smart devices are used for professional purposes, such as authentication, learning activities, recording rewards or sanctions, or other agreed tasks, I will use school-provided devices where available. Where staff are permitted to use personal devices for professional purposes, such as communication on a school trip and authentication, this must be formally agreed by the school and managed in line with school policy.
30. 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 or other designated leader. Use must not compromise supervision, safeguarding, confidentiality, professional boundaries, data protection or the learning environment.

Online communication, including use of social media

31. 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.
32. I will protect myself, my professional reputation and the reputation of the school online. I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.
33. My electronic communications with current and former pupils and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
 - I will ensure that all electronic communications take place in a professional manner via school-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 pupils 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 pupils, such as my personal address, email address or phone number.
 - I will not share personal information about my private life with pupils 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 pupils, 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 pupils, staff and the wider school community by ensuring professional boundaries, safeguarding expectations and communication arrangements are clear.
 - Where digital communication with pupils or families is required, I will follow the school's expectations about when communication should take place, including any agreed arrangements for out-of-hours contact, emergency communication or role-specific responsibilities.

Policy concerns

34. 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.
35. 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.

36. 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.
37. I will report and record any concerns about the welfare, safety or behaviour of pupils or parents/carers online to the DSL in line with the school child protection policy.
38. 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 Code of Conduct and Whistleblowing Policy.

Policy compliance and breaches

39. 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/or the headteacher.
40. 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 pupils and staff.
 - This includes monitoring all school-provided devices and school systems and networks including school-provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school-provided devices, systems and/or networks.
 - This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
 - Staff will be informed about the nature, purpose and extent of monitoring through this AUP, relevant policies, privacy information and/or staff guidance.
41. 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 Code of Conduct].
42. 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 headteacher so it can be recorded and managed transparently.
43. 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 headteacher and/or DSL without delay, even if it appears minor, accidental or unlikely to meet the harm threshold.
44. 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 Child Protection, Staff Code of Conduct, Whistleblowing, 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.

45. 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.
46. I understand that if the school suspects criminal offences have occurred, the police will be informed where appropriate.
47. 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 DSL and/or headteacher before taking action. I will act in a way that safeguards pupils, protects professional boundaries, and is open to scrutiny.

I have read, understood and agreed to comply with Claremont'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

Visitors, Volunteers and Contractors Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, it is important that visitors and volunteers understand our expectations for safe, lawful and responsible technology use while on site, when using school systems, or when acting in a role connected to the school. This AUP helps Claremont Primary School explain expectations around safeguarding, professional conduct, data protection, image use, mobile phones, online communication and reporting concerns.

Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems, services, devices or information provided by the [school/setting], or accessed by me as part of my role, visit or activity with Claremont Primary School. It also applies to personal devices or accounts where their use takes place on site, involves the school community, is linked to my role or visit, or could affect safeguarding, confidentiality, data protection, professional boundaries or the reputation of the school.
2. I understand that this AUP should be read and followed in line with relevant school policies, including the Information for Volunteers, Memorandum of Understanding, Child Protection Policy, Image Use Policy and Mobile & Smart Phone Technology Policy.
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, including but not limited to child sexual abuse material, criminally racist material, terrorist material or adult pornography covered by the Obscene Publications Act.
5. 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, where this takes place on school premises, during my visit/volunteering activity, or in any context linked to my role.
6. I will not engage in any online activity, digital communication or behaviour that could compromise safeguarding, professional boundaries or the reputation of the [school/setting].

Data and image use

7. Where I have access to personal data, confidential information, safeguarding information, school systems, records or devices, I will only access, use or share this information where it is necessary for my agreed role, visit or activity and in line with data protection legislation and school procedures. I will not copy, download, photograph, record, forward or share information unless this has been authorised.

8. I will not take, use, store or share images or recordings of pupils during lessons, visits, trips, events, performances, activities or celebrations unless this has been specifically authorised by the school and is in line with the school Image Use Policy. Where authorised, images or recordings must only be taken, used, stored or shared using school approved equipment, accounts and systems, unless leaders have made a specific, risk-assessed decision otherwise. I will not take images or recordings of pupils for personal use or share them on personal devices, personal accounts, social media, messaging apps or online groups.

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 pupils .
10. Where I am supporting pupils , I will reinforce safe and appropriate technology use and will follow staff instructions and school policies.
11. 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 a Designated Safeguarding Lead (DSL), in line with the school Child Protection Policy.
12. 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.
13. I will not record, transcribe, livestream, use AI note-taking tools, recording bots or automated meeting summary tools during any meeting, visit, lesson, activity or professional discussion unless this has been specifically authorised by the school and is in line with safeguarding, confidentiality, consent and data protection expectations.

Use of mobile phones and smart devices

14. In line with the school Mobile & Smart Phone Technology Policy, I will model safe and appropriate use of mobile phones and smart devices while on site. I will not use or have visible my own mobile phone or smart device in front of pupils unless this has been agreed by the school and is directly linked to my role, visit or volunteering activity. I will follow the school's expectations about where and when mobile phones and smart devices may be used or stored.

Online communication, including the use of social media

15. I will ensure that my online conduct, reputation and use of technology are 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.
16. Any electronic communication with pupils, parents/carers or staff as part of my role, visit or volunteering activity will take place within clear professional boundaries and be transparent and open to scrutiny.
 - Communication will take place using school approved channels, such as a school-provided email address, account, platform or telephone number.
 - I will not use personal devices, personal email, personal social media, private messaging apps, gaming accounts or personal phone numbers to contact pupils

or their families unless this has been formally approved, risk assessed and recorded by leaders.

- Any pre-existing relationships, links or situations that may affect how I apply this AUP will be discussed with the DSL and/or headteacher.
17. I will respect confidentiality and will not post, comment on, discuss or share information online about pupils, staff, families, incidents, activities or anything I become aware of through my role, visit or volunteering activity. This includes comments, images, videos, recordings or information shared on personal social media, messaging apps, online groups or community forums.

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 [Clare Smith] and/or the headteacher.
19. 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 pupils and staff.
- This includes monitoring all school-provided devices and school systems and networks, including school-provided internet access, whether used on or offsite, and may include the interception of messages and emails sent or received via school-provided devices, systems and/or networks.
 - This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.
20. I will report and record any concerns about the welfare, safety or behaviour of pupils or parents/carers online to the DSL, in line with the school Child Protection Policy.
21. I will report concerns about the welfare, safety, conduct or behaviour of staff, including online, digital, device-related, image-related or technology-linked concerns, to the headteacher, in line with the school child protection policy, staff behaviour/code of conduct, low-level concerns procedures and/or allegations against staff policy.
22. I understand that if the school believes that illegal, unauthorised or inappropriate use, unacceptable behaviour, or a breach of this AUP has taken place, action may be taken in line with relevant safeguarding, behaviour, complaints, volunteer, contractor, visitor, data protection, low-level concerns or allegations procedures, as appropriate. This may include ending or restricting access to the site, systems or activities, informing an employer/agency/organisation, seeking advice from the LADO, informing the DPO/data protection lead, or contacting the police where appropriate.
23. 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 headteacher without delay, even if it appears minor, accidental or unlikely to meet the harm threshold.
24. Where a concern involves personal data, confidential information, safeguarding information, images, recordings, AI tools, transcription tools or unauthorised sharing, the Data Protection Officer (DPO) will be informed promptly so that any data protection, information governance or reporting requirements can be considered.

25. 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 DSL and/or headteacher.

I have read, understood and agreed to comply with Claremont’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

Wi-Fi Acceptable Use Policy

All visitors accessing the Guest Wi-fi are required to read the following and accept the terms via their device.

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 provides Wi-Fi for visitors who need Wi-Fi access in order to carry out their role e.g. NHS staff, contractors, music teachers.
2. Use of the Wi-Fi falls under Claremont Primary School's Acceptable Use of Technology Policy (AUP), the Child Protection Policy, Positive Behaviour Policy, Data Protection policies and any other relevant policies. All pupils, 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 school 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 Lead (Clare Smith) or identified technical contact as soon as possible. If I have any queries about safe behaviour online, I will speak to the DSL 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, employer/organisation, LADO or police.

I have read, understood and agreed to comply with Claremont's Wi-Fi Acceptable Use Policy

Name

Signed

Date