



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 2025
Date of next review	Autumn 2026
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 Wi-Fi on their personal devices while on the premises. Paragraphs about the use of the Wi-Fi 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 online.
- I only go online when an adult is with me
- I only click on things online 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 polite and friendly messages online
- I know the school can see what I am doing online when I use 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 only send messages which are polite and friendly
- I will only share pictures or videos online if they are safe, kind, and I have asked for permission first.
- I will only click on links if a trusted adult says they are safe.
- I know that people online might not be who they say they are. I will only chat with people I know or who a trusted adult says are safe.
- If someone online asks to meet me, I will tell a trusted adult straight away.

Learning

- I always ask permission from an adult before using the internet.
- I only use websites, tools and/or search engines that my teacher has chosen or given me permission to use.
- I use 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
- I will use Artificial Intelligence (AI) tools safely and sensibly. I won't use them to cheat, copy other people's work or say anything unkind. I know that AI tools can sometimes make mistakes. I will only use them when a teacher or trusted adult says it's OK.

Trust

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

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.
- If I am in Year 6 and bring my 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 will only change the settings on the computer if a teacher has allowed me to

Tell

- If I see anything online that I should not or I see something online that makes me feel worried or upset, I will report it to a teacher or other adult.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher or other adult.
- I know it is not my fault if I see something upsetting or unkind online.
- If I'm not sure about something online or it makes me feel worried or scared, I will talk to a trusted adult.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all school owned devices are checked 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 for any reason, I need to bring a person device into school, like a smartphone or wearable technology, I will need permission from Mrs Roberts. If I am in Year 6 and bring my phone to school, I will hand it in at the beginning of the day to the adults in my class. I will not use it at all once I am inside the school gates. I will keep it turned off when I am in school, unless an adult has given me permission to turn it on.
- 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 red card. They will also talk to my parents.
- I have read and talked about these rules with my parents/carers

- I understand that online incidents that occur outside of school may also be picked up inside of school to support everyone.

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

1. I, with my child, have read and discussed Claremont's pupil Acceptable Use of Technology policy (AUP). I understand that the aim of the AUP is to help keep my child safe online.
2. I understand that the AUP applies to my child's use of school devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another child, could have repercussions for the orderly running of the school, if a child is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.
3. I understand that any use of school devices and systems are appropriately filtered. Claremont's education broadband connectivity is provided through PJA Systems and Claremont uses Netsweeper. We work with Cantium Business Solutions and PJA Systems Limited to ensure that our filtering policy is continually reviewed to reflect our needs and requirements
4. I am aware that my child's use of school provided devices and systems will be monitored for safety and security reasons. 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. I however understand that the school/setting cannot ultimately be held responsible for filtering breaches that occur due to the dynamic nature of materials accessed online, or if my child is using a personal device, including mobile or smart technologies
6. I am aware that the school policy states that my child cannot use personal devices on site. This includes smart watches, tracking devices and any other internet-enabled device. Only Year 6 pupils may bring mobile phones on site and these are kept in a locked box in the classroom during the school day. My child is not allowed to use their phone once they have entered the school site and I have discussed this with them.
7. I understand that my child needs a safe and appropriate place to access remote learning, for example if the school is closed. I will ensure my child's access to remote learning is appropriately supervised. When accessing video learning, I will ensure they follow the protocols outlined in the Acceptable Use of Technology Addendum.
8. I, and my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

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 the Designated Safeguarding Lead or one of their Deputies) or other relevant organisations if I have concerns over my child’s or other members of the school communities’ 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’s online safety approaches and safeguarding my child and other children. This includes my use of phones/devices on school site.
13. I will use parental controls and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding. I know that I can speak to the Designated Safeguarding Lead (Clare Smith), my child’s teacher or the headteacher if I have any concerns about online safety.

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 Claremont IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for pupils, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand Claremont's expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy Scope

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

Use of School Devices and Systems

4. I will only use the equipment and internet services provided to me by the school (for example, school provided laptops, tablets, mobile phones and internet access) when working with children, unless I have permission from the headteacher for a specific reason.
5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and other professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems by staff is allowed during break and lunchtimes away from children. This is at the school's discretion and can be revoked at any time.

Data and System Security

6. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.

- I will use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system.
 - 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.
7. I will respect school system security and will not disclose my password or security information to others.
 8. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager.
 9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.
 10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school information security policies.
 - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
 - Any data being removed from the school site, such as via email hard drives will be suitably protected. All hard drives used must be encrypted.
 - Any data being shared online, such as via cloud systems or artificial intelligence tools (AI), will be suitably risk assessed and approved by the schools' Data Protection Officer and leadership team prior to use to ensure it is safe and legal.
 11. I will not keep documents which contain school related sensitive or personal information, including images, files, videos and emails, on any personal 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.
 12. 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.
 13. 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.
 14. I will not attempt to bypass any filtering and/or security systems put in place by the school.

15. 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.
16. 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 (Colin Howard, Satswana) as soon as possible.
17. Any images or videos of pupils will only be used as stated in the school image use policy. I understand images of pupils must always be appropriate and should only be taken with school provided equipment and taken/published where pupils and their parent/carer have given explicit written consent.

Classroom Practice

18. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by Claremont as detailed in the Child Protection and Safeguarding Policy and as discussed with me as part of my induction and ongoing safeguarding and child protection staff training.
19. 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, in line with the school's Child Protection and Safeguarding policy.
20. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces, including appropriate supervision of pupils, as outlined in the school Child Protection and Safeguarding Policy and AUP and Online Safety addendums.
21. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I also recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material. Additionally, its use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that:
 - The approved AI platform for Claremont is TeachMate AI.
 - AI tools are only to be used responsibly and ethically, and in line with our school/college child protection, data protection, and professional conduct/behaviour policy expectations.
 - A risk assessment will be undertaken, and written approval will be sought from the senior leadership team prior to any use of AI tools, for example if used in the classroom, or to support lesson planning.
 - A Data Protection Impact Assessment (DPIA) will always be completed prior to any use of AI tools that may be processing any personal, sensitive or confidential data and use will only occur following approval from the DPO.
 - I am required to critically evaluate any AI-generated content for accuracy, bias, and appropriateness before sharing or using it in educational contexts.
 - AI must not be used to replace professional judgement, especially in safeguarding, assessment, or decision-making involving pupils.

- 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.
 - Any misuse of AI will be responded to in line with relevant school/college policies, including but not limited to, anti-bullying, staff and pupil behaviour and child protection.
22. 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 on site.
 - creating a safe environment where pupils 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) (Clare Smith) or a deputy (Candi Roberts/ Sarah Seddon) 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 DSL and /or deputies if I am teaching topics which could place unusual activity on 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 pupils is appropriate.
23. 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 or use them.

Mobile Devices and Smart Technology

24. I have read and understood the school's Child Protection and Safeguarding Policy and staff code of conduct which cover expectations regarding staff use of mobile technology and social media.
25. 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 Child Protection and Safeguarding policy and the law.

Online Communication, including use of social media

26. I will ensure that my use of communication technology, including use of social media is compatible with my professional prole, does not interfere with my work duties and takes place in line with the staff code of conduct, the Child Protection and Safeguarding policy and the law.

- 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 as outlined in the Child Protection Policy and staff code of conduct.
 - I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.
 - I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the school code of conduct and the law.
27. My electronic communications with current and past pupils and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
28. As outlined in the Staff Code of Conduct:
- I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels, such as a school email address or telephone number. All emails to parents will be sent via the admin email address.
 - I will not share any personal contact information or details with pupils, 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 pupils and/or parents/carers.
 - If I am approached online by a pupil or parents/carer, I will not respond and will report the communication to my line manager and Clare Smith, Designated Safeguarding Lead (DSL).
 - Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the headteacher.

Policy Concerns

29. 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.
30. 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.
31. 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.
32. I will report and record concerns about the welfare, safety or behaviour of pupils or parents/carers to the DSL via CPOMS in line with the school child protection and safeguarding policy.
33. I will report concerns about the welfare, safety or behaviour of staff to the Headteacher, in line with the Whistleblowing Policy.

Policy Compliance and breaches

34. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the DSL and/or the headteacher.
35. 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.
36. 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 discipline and conduct policy.
37. 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 discipline and conduct policy.
38. 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 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 children's safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of their professional responsibilities when using technology. This AUP will help Claremont ensure that all visitors and volunteers understand the school's expectations regarding safe and responsible technology use.

Policy Scope

39. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services provided to me or accessed as part of my role within Claremont both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras and email as well as IT networks, data and data storage and communication technologies.
40. I understand that Claremont's AUP should be read and followed.
41. 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.
42. 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.
43. 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.
44. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school/setting into disrepute.

Data and Image Use

45. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including UK GDPR.
46. I understand that I am not allowed to take images or videos of pupils.

Classroom Practice

47. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of pupils, as outlined in the school online safety policy.
48. I will support teachers in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the children I am supporting.
49. I will immediately report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the Designated Safeguarding Lead (DSL) (Clare Smith) in line with the school child protection and safeguarding policy.

50. Where I deliver or support remote learning, I will comply with the school's remote learning AUP.
51. 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, distribute or use it.

Use of Mobile Devices and Smart Technology

52. I have read and understood the school Child Protection policy which covers expectations regarding use of social media, mobile devices and smart technology.
53. I understand that the school requires 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, it must be used in an area where no pupils are present and a member of the SLT advised.

Online Communication, including the Use of Social Media

54. 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 not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.
 - I will take appropriate steps to protect myself online.
 - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in according with the school's code of conduct, online safety policy and within the law.
55. My electronic communications with pupils, 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 this will be discussed with the DSL (Clare Smith) or the Headteacher (Candi Roberts).

Policy Compliance, breaches or concerns

56. 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 Designated Safeguarding Lead (Clare Smith) or the headteacher.
57. 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.

58. 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.
59. 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.
60. I understand that the school may exercise its right to monitor the use of school information systems, including internet access and the interception of emails/messages on school systems to monitor policy compliance and to ensure the safety of learners, staff and visitors/volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.
61. I will report and record concerns about the welfare, safety or behaviour of pupils or parents/carers to the Designated Safeguarding Lead (Clare Smith) in line with the school child protection and safeguarding policy.
62. I will report concerns about the welfare, safety or behaviour of staff to the headteacher, in line with the whistleblowing policy.
63. I will report concerns about the welfare, safety or behaviour of staff online to the headteacher, in line with the whistleblowing policy.
64. I understand that is 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.
65. 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 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 (for training courses only) are required to read the following and accept the terms via their device. Other visitors/volunteers to not have access to the school wi-fi.

As a professional organisation with responsibility for children's safeguarding, Claremont School believes it is important that all members of the community, including visitors, are fully aware of the school boundaries and requirements when using the school Guest 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, including visitors, are reminded that technology use should be consistent with our ethos, other appropriate policies and the law.

1. The school provides Guest Wi-Fi for the school for visitors attending training courses 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/setting premises that is not the property of the school.
3. The use of technology falls under Claremont's Acceptable Use of Technology Policy (AUP), online safety policy, staff code of conduct and positive behaviour policy which all pupils, 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 Guest Wi-Fi 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 Guest 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 (Clare Smith) as soon as possible.
14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (Clare Smith) or the headteacher.
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 Claremont's Wi-Fi Acceptable Use Policy

Name

Signed

Date