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	Rachel Daly/Rob Jackson Safeguarding governors
Responsible governor team	FGB
Date approved	March 2024
Date of next review	Spring 2025
Policy reference	Adopted KCC/The Education People V1: published August 2023

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

Pupil Acceptable Use of Technology

Early Years and Key Stage 1 (0-6)

- I understand that the school Acceptable Use Policy (AUP) will help keep me safe and happy online.
- I only use the internet when an adult is with me.
- I only click on online links and buttons when I know what they do. If I am not sure, I ask an adult first.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online when I use school computers/iPADs including if I use them at home.
- I always tell an adult/teacher/member of staff if something online makes me feel upset, unhappy, or worried.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online.
- I know that if I do not follow the school rules:
    - I will need to speak with an adult and a consequence may follow
    - My parents will be informed
- I have read and talked about these rules with my parents/carers.

Key Stage 2 (7-11)

I understand that the school Acceptable Use Policy (AUP) will help keep me safe and happy online at home and at school.

Safe

- I will behave online the same way as I behave in the classroom.
- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are safe and appropriate, and **if I have permission**.
- I only talk with, and open messages, from people I know.
- I will only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

Learning

- At Claremont I know we use computers, laptops, iPADs and can store documents on the Pupil Shared Drive. I must only save things that my teachers has asked me to save.
- The use of my own personal smart devices and/or mobile phone at school is not permitted and if I bring my own devices to school, it must be handed to an adult at the start of the day and collected at the end of the day.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.

- I use school devices for school work unless I have permission otherwise.
- If I need to learn online at home, I will follow the school remote/online learning AUP.

Trust

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

Responsible

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

Tell

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

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all school owned devices and networks are monitored to help keep me safe, including if I use them at home. This means someone at the school may be able to see and/or check my online activity when I use school devices and/or networks if they are concerned about my or anyone else's safety or behaviour.
- The use of my own personal smart devices and/or mobile phone at school is not permitted and if I bring my own devices to school it must be handed to an adult at the start of the day and collected at the end of the day.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online or to see help.
- I know that if I do not follow the school rules then:
  - I will need to speak with one of the DSLs and a consequence may follow.
  - My parents will be informed.

Pupils with Special or additional Educational Needs

- I ask a grown-up if I want to use the computer.
- I make good choices on the computer.
- I use kind words on the internet.
- If I see anything that I do not like online, I tell a grown up.
- I keep my information private on the internet.
- With permission, I am careful if I share photos online.
- I know that if I do not follow the school rules then:
  - I will need to speak with an adult I know well, and a consequence may follow.
  - My parents will be informed.

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 Acknowledgement Form

1. I have read and discussed Claremont's pupil acceptable use of technology policy (AUP) with my child and understand that the AUP will help keep my child safe online.

2. I understand that the AUP applies to my child's use of Claremont devices and systems on site and at home including mobile phones, gaming consoles, iPADs, computers and laptops, 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 Claremont, 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; this means/includes filtering and monitoring systems. (See Claremont Child Protection Policy Addendum Feb 2024)

4. I am aware that my child's use of school provided devices and systems will be monitored for safety and security reasons, when used on and offsite. This includes appropriate monitoring systems. Monitoring approaches are in place to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

5. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use school devices and systems, on and offsite. I however understand that the school cannot ultimately be held responsible for filtering breaches that occur due to the dynamic nature of materials accessed online, or if my child is using a personal device, including mobile or smart technologies.

6. I am aware that the school Child Protection Policy states that my child cannot use personal devices, including mobile and smart technology on site.

7. I understand that my child needs a safe and appropriate place to access remote/online learning, for example, if the school is closed. I will ensure my child's access to remote/online learning is appropriately supervised and any use is in accordance with the school use of TEAMs for remote learning procedures.

8. I and my child are aware of the importance of safe online behaviour and will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the school community, or content that could adversely affect the reputation of the school.

9. I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety online.

10. I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school community's safety online. Mrs Seddon (Deputy DSL: Online Safety)

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 schools online safety approaches and safeguarding my child online. I will use parental controls, supervise access and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Child's Name ………………………………………………………………………………………………….

Child's Signature ………………………………………………………………………………….. *(If in KS2)*

Class ………………………………………………………………………………………………………..

Date ……………………………………………………………………………………………………

Parent/Carer's Name …………………………………………………………………………………..

Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Claremont Primary School 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 Primary School expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school or accessed by me as part of my role within Claremont Primary School, professionally and personally, both on and offsite. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email. data and data storage, remote learning systems and communication technologies.

2. I understand that Claremont Primary School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school child protection/online safety policy 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, 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 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/or 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 use at the school's discretion and can be revoked at any time.

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

Data and system security

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

    -   I will use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters and does not contain a dictionary word.
    -   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.

8. I will respect school system security and will not disclose my password or security information to others.

9. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager.

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

11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK GDPR in line with the school information security policies.

    -   All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    -   Any data being removed from the school site, such as via email or on memory sticks or hard drives will be suitably protected. All memory sticks and hard drives used must be encrypted.

12. I will not keep documents which contain school related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school learning platform to upload any work documents and files. 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.

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

14. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to

computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

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

16. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Support Provider (Paul Ashmore) as soon as possible.

17. 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 (Julie Cook) as soon as possible.

18. Any images or videos of pupils will only be used as stated in the school camera and image use policy . I understand images of pupils must always be appropriate and should only be taken with school provided equipment and only be taken/published where parent/carers have given explicit written consent.

Classroom practice

19. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by Claremont Primary School as detailed in Claremont Child Protection/ online safety Policy, and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training. I know that Sarah Seddon (DDSL) holds responsibility for online Safety and the first point of contact)

20. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT provider: Paul Ashmore- PJA Systems, in line with the school child protection/online safety policy.

21. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces such as the Computer suite. Link to CP Policy.

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 leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
- make informed decisions to ensure any online safety resources used with pupils is appropriate.

23. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

Mobile devices and smart technology

24. 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/Online Safety and the law.

Online communication, including use of social media

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

26. As outlined in the Staff Code of Conduct:
    o 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.
    o I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.

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.
    o 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.
    o I will not share any personal contact information or details with pupils, such as my personal email address or phone number.
    o I will not add or accept friend requests or communications on personal social media with current or past pupils and/or parents/carers.
    o 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).
    o Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the headteacher.

Policy concerns

28. 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.

29. 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.

30. 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.

31. I will report and record concerns about the welfare, safety or behaviour of pupils or parents/carers to the DSL in line with the school child protection and safeguarding policy.

32. 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

33. 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.

34. 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 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.

35. I understand that if the school believe that unauthorised and/or inappropriate use of school devices, systems or networks is taking place, the school may invoke its disciplinary procedures as outlined in the Staff Code of Conduct/Discipline & Conduct Policy.

36. 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 & Conduct policy.

37. 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 Primary School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member ……………………………………………………………………………..

Signed ……………….…………………………………………………………………………….

Date (DDMMYY) ……………………………………………………………………………..

Visitor and Volunteer Acceptable Use of Technology Policy

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

Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school or accessed by me as part of my role within Claremont Primary School, professionally and personally. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email data and data storage, remote learning systems and communication technologies

2. I understand that Claremont Primary School AUP should be read and followed in line with the school staff code of conduct 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, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

5. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

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

Data and image use

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

Classroom practice

8. 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 Child Protection Policy.

9. I will support and reinforce safe behaviour whenever technology is used on site and I will promote online safety with the pupils I am supporting.

10. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the school community, I will report this to the

DSL and/or HT who will inform Claremont's IT provider Paul Ashmore- PJA Systems- in line with the school child protection/online safety policy.

11. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music is protected, I will not copy, share, or distribute or use it.

Use of mobile devices and smart technology

Online communication, including the use of social media

12. 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.
    o I will take appropriate steps to protect myself online as outlined in the Child Protection/Online Safety.
    o I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.
    o I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the school code of conduct/behaviour policy and the law.

1. 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.
    o All communication will take place via school approved communication channels such as via a school provided email address, account or telephone number.
    o Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
    o 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

13. 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.

14. 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 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.

15. I will report and record concerns about the welfare, safety or behaviour of pupils or parents/carers online to the Designated Safeguarding Lead (Clare Smith) in line with the school child protection policy.

16. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with the allegations against staff policy.

17. I understand that if the school believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.

18. 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 Primary School visitor/volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer …………………………………………………………………...……………

Signed ……………………………………………………………………………………………………….

Date (DDMMYY) …………………………………….......………………………………………………...

Wi-Fi Acceptable Use Policy

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 it is important that all members of the school community are fully aware of the school boundaries and requirements when using the school Wi-Fi systems and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

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

1. The school provides Wi-Fi for the school community and allows access for visitors attending training courses.

2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the school premises that is not the property of the school.

3. The use of technology falls under Claremont's Acceptable Use of Technology Policy (AUP), Child Protection/Online Safety policy 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 wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my

sole responsibility; and I indemnify and hold harmless the school from any such damage.

9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

10. I will not attempt to bypass any of the school security and filtering systems or download any unauthorised software or applications.

11. My use of school 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 Primary School Wi-Fi Acceptable Use Policy.

Name ……………………………………………………………………………………………………..

Signed ……………………………………………………………………………………………………..

Date (DDMMYY) ……………………………………………………………………………………..

Additional information and guides on specific platforms can be found at:
- LGfL: Safeguarding Considerations for Remote Learning
- SWGfL: Which Video Conference platform is best?

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