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	Matt Lowe, Safeguarding governor
Responsible governor team	FGB
Date approved	March 2022
Date of next review	Spring 2023
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 Online Safety 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, we ask that it is used in areas where no pupils are present.**
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 only use the internet when an adult is with me
- I only click on links and buttons online when I know what they do
- 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
- I use the iPads for what I have been asked and I use my allocated iPad
- I always tell an adult if something online makes me feel unhappy or worried
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online
- If I need to learn online at home, I will follow the school's online safety rules outlined in the Covid-19 AUP addendum.
- 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 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 only click on links if I know they are safe
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.
- I talk to an adult if somebody says something that makes me feel uncomfortable online
- If I need to learn online at home, I will follow the school's online safety rules outlined in the Covid-19 AUP addendum.

Learning

- I always ask permission from an adult before using the internet.
- I only use websites that my teacher has recommended and I use SafeSearch as a search engine.
- 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

- If I need to learn online at home, I will follow the school remote learning AUP.

Trust

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

Responsible

- I keep my personal information safe and private online
- I will keep my passwords safe and not share them with anyone
- 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 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

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of school devices/computers and internet access are monitored to help keep me safe.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online
- I have read and talked about these rules with my parents/carers

Tell

- 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 or someone sends me something bad online. I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page or app and tell an adult straight away.

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.

3. I understand that my child needs a safe and appropriate place to access remote learning if the school is closed in response to Covid-19. 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.

4. I am aware that any internet and IT use using school equipment may be monitored for safety and security reason to safeguard both my child and the school systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

5. I am aware that the school policy states that my child cannot use personal devices on site. 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.

6. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child will be safe when they use the internet and other associated technologies. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
7. I will support school safeguarding policies and will ensure that I appropriately monitor my child's use of the internet outside of school and discuss online safety with them when they access technology at home.

8. I with 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 will support the School online safety approaches. 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…….....

Parents Signature……... 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. 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 the Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school's 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 (which may be necessary when providing remote learning as a result of school closures in the response to Covid-19).

5. I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff. Reasonable person use of setting IT systems by staff is allowed during break and lunchtimes away from children.

6. Where I deliver or support remote learning, I will comply with the school's 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 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 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.

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 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 consent.

Classroom Practice

19. 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 online safety policy and AUP and Online Safety addendums.

20. I have read and understood the school online safety policy which covers expectations for pupils regarding mobile technology and social media.

21. 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.
    - make informed decisions to ensure any online safety resources used with pupils is appropriate.

22. I will report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the DSL in line with the school child protection policy.

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 have read and understood the school online safety policy which covers 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 online safety 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 comptatible with my professional prole, does not interfere with my work duties and takes place in line with the staff code of conduct, the online safety policy and the law. In lin with the school online safety policy and staff code of conduct:
    - I will take appropriate steps to protect myself and my reputation online when using communication technology including the use of social media as outlined in the online safety policy.
    - 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.
    - 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

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 is 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 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 information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of pupils and staff. 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 systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the staff discipline and 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 and 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'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 (DDMMYY)……...

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

1. 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**.**

2. I understand that Claremont's AUP should be read and followed.

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.

Data and Image Use

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

Classroom Practice

5. 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.

6. 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.

7. 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 policy.

8. Where I deliver or support remote learning, I will comply with the school's remote learning AUP.

9. 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

10. I have read and understood the school online safety policy which covers expectations regarding use of social media, mobile devices and smart technology.

Online Communication, including the Use of Social Media

11. 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.

12. 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 this will be discussed with the DSL (Clare Smith) or the Headteacher.

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 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.

15. 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.

16. 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.

17. 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 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.

18. 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 policy.

19. I will report concerns about the welfare, safety or behaviour of staff to the headteacher, in line with the whistleblowing policy.

20. 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.

21. 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 (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 safeguarding, Claremont School believes it is important that visitors understand the risks involved with the use of mobile phones and devices on the school site.

Most mobile phones and devices now include a camera facility, and this allows photographs to be taken with ease in any location. 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.

1. The school provides Guest Wi-Fi for the school for visitors attending training courses only.
2. I am aware that the school/setting 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/setting.
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 learners/staff/visitors and volunteers must agree to and comply with.
4. The school/setting 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/setting 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/setting service is adequately secure, such as up-to-date anti-virus software, systems updates.
7. The school Guest WiFi 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/setting 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.