



Acceptable Use Policy

"I am able to do all things through Him who strengthens me" Phillippians 4:13

By: Mrs E Pearson

Review: Governors Meeting 20/11/2024

Next: November 2025

Contents

Child Acceptable Use of Technology Sample Statements..... 3

 Early Years and Key Stage 1 (0-6)..... 3

 Key Stage 2 (7-11) 3

Children with Special Educational Needs and Disabilities (SEND) 5

Staff Acceptable Use of Technology Policy (AUP)..... 9

 Visitor and Volunteer Acceptable Use of Technology Policy..... 15

 Wi-Fi Acceptable Use Policy..... 18

Remote/Online Learning AUP Template - Staff Statements 19

Acknowledgements and Thanks 20

We cultivate a rich environment in all we do so that the school community, have the right to Learn, Enjoy, Grow, developing spiritually and having awe-inspiring learning experiences. Our children learn within a culture of acceptance, build resilience and flourish in unique ways, underpinned through the teachings of Jesus, through God and in his world.

Child Acceptable Use of Technology

Early Years and Key Stage 1 (0-6)

- I understand that the Teynham CE Primary School Acceptable Use Policy will help keep me safe and happy online.
- I only use the internet when an adult is with me.
- I only click on online links and buttons when I know what they do. If I am not sure, I ask an adult first.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online when I use school computers and Ipads
- I always tell an adult if something online makes me feel upset, unhappy, or worried.
- I can visit www.ceopeducation.co.uk or www.thinkuknow.co.uk to learn more about keeping safe online.
- I know that if I do not follow the school rules:
 - My parents/carers will be informed
- I have read and talked about these rules with my parents/carers.

Shortened KS1 version (for use on posters or with very young children)

- I only go online with a grown-up.
- I am kind online.
- I keep information about me safe online.
- I tell a grown-up if something online makes me unhappy or worried.

Key Stage 2 (7-11)

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

Safe

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

Learning

- I will use all school devices with appropriately and with care
- I will store my work on the pupil shared drive
- AI may be used through secure channels with adult supervision
- Mobile phones have to be given to the office at the start of the school 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.
- If I need to learn online at home, I will follow the school 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 minimise the screen and tell an adult immediately.
- If I am aware of anyone being unsafe with technology, I will report it to an adult at school.
- I know it is not my fault if I see, or someone sends me, something upsetting or unkind online.
- I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all school owned devices and networks are monitored to help keep me safe. This means someone at the school may be able to see and/or check my online activity when I use school devices and networks if they are concerned about my or anyone else's safety or behaviour.
- If, for any reason, I need to bring a personal device, for example a smart/mobile phone and/or other wearable technology into school then I will hand it to the school office at the start of the day.
- I have read and talked about these rules with my parents/carers.

- I can visit www.ceopeducation.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:
 - My parents/carers will be informed

Shortened KS2 version (for use on posters)

- I ask an adult about which websites I can use.
- I will not assume information online is true.
- I know there are laws that stop me copying online content.
- I know I must only open online messages that are safe. If I am unsure, I will not open it without speaking to an adult first.
- I know that people online are strangers, and they may not always be who they say they are.
- If someone online suggests meeting up, I will always talk to an adult straight away.
- I will not use technology to be unkind to people.
- I will keep information about me and my passwords private.
- I always talk to an adult if I see something which makes me feel worried.
- I know my use of school devices and systems can be monitored.

Children with Special Educational Needs and Disabilities (SEND)

Safe

- I ask a grown up if I want to use the computer.
- I do not tell strangers my name on the internet.
- I know that if I do not follow the school rules then:
 - My parents will be informed

Meeting

- I tell a grown-up if I want to talk on the internet.

Accepting

- I do not open messages or emails from strangers.

Reliable

- I make good choices on the computer.

Tell

- I use kind words on the internet.
- If I see anything that I do not like online, I will tell a grown up.

Acceptable Use of Technology for Parents/Carers

Teynham CE Primary School Child Acceptable Use of Technology Policy

Acknowledgment

1. I have read and discussed Teynham CE Primary School's child acceptable use of technology policy (AUP) with my child and understand that the AUP will help keep my child safe online.
2. I understand that the AUP applies to my child's use of school devices and systems on site and at home including, 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; this includes regular monitoring from IT support.
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 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.
6. I am aware that the school mobile and smart technology policy states that my child cannot use personal devices, including mobile and smart technology on site. Mobile phones should be switched off and handed to the office at the start of the day.
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 AUP. Remote learning would be using school-based websites that the children already use for homework. For example – Nessy or TT Rock Stars
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 by informing the Class Teacher or a member of SLT I have concerns over my child's or other members of the school community's safety online.
11. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.
12. I understand my role and responsibility in supporting the school's 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.

Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use the school's 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 children, 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 expectations regarding Teynham CE Primary School's 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 Teynham CE 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 Teynham CE Primary School's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the Teynham, Child Protection and Safeguarding Policy, Code of Conduct, Mobile Technology and Social Media Policy and KCSIE.
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 code of conduct 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.
5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and devices by staff is allowed. Occasional personal use of the settings devices could be considered as beneficial to the development of staff IT skills and can enable staff to maintain a positive work-life balance. However, this is at the setting's discretion and can be revoked at any time.

6. Where I deliver or support remote/online learning, I will comply with the school AUP. I will follow all policies (code of conduct, Teynham Child Protection and Safeguarding) to ensure the safety of the children.

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 locking access.
- I will use a 'strong' password to access school systems. Passwords are changed regularly when prompted by the network.
 - I will protect the devices in my care from unapproved access or theft. I will not leave any devices visibly in a public place.
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 EIS
10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the EIS.
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 CDs, will be suitably protected. This may include data being encrypted by a method approved by the school.
 - Any data being shared online, such as via cloud systems or artificial intelligence tools (AI), will be suitably risk assessed and approved by the school Data Protection Officer and leadership team prior to use to ensure it is safe and legal.
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 (access to school email on mobile phones is permitted as long as this is password protected)
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's 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 Headteacher and IT support as soon as possible.
17. If I have lost any school related documents or files related to GDPR regulations, I will report this to IT support and school Data Protection Officer (Corinne Murray) as soon as possible.
18. Any images or videos of children will only be used as stated in the school Photography policy and consent. I understand images of children must always be appropriate and should only be taken with school provided equipment and only be published where children's 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 Teynham CE Primary School as detailed in Teynham Child Protection and Safeguarding, Mobile Technology and Social Media Policies and as discussed with me as part of my induction and ongoing safeguarding and child protection staff training.
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, in line with the school's Child Protection and Safeguarding Policy and Mobile, Smart Technology and Social Media Policy.
21. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in, for example, Teynham Child Protection and Safeguarding Policy, Mobile, Smart Technology and Social Media Policy and remote learning AUP.
22. 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 use of AI as part of our curriculum approaches is not permitted by staff and pupils.
 - 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 or assessments).
 - Any misuse of AI will be responded to in line with relevant school policies, including but not limited to, Anti-bullying, Staff Code of Conduct, Positive Behaviour, Teynham Child Protection and Safeguarding and Mobile, Smart Technology and Social Media Policies.

23. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
- exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
 - creating a safe environment where children feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
 - involving the Designated Safeguarding Lead (DSL) (Mrs E Pearson) or a deputy (Mrs C Murray and Mrs E Butler) as part of planning online safety lessons or activities to ensure support is in place for any children who may be impacted by the content.
 - Informing the DSL and leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
 - make informed decisions to ensure any online safety resources used with children is appropriate.
24. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

Mobile devices and smart technology

25. I have read and understood the school mobile and smart technology and social media policies which addresses use by children and staff.
26. 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 code of conduct and the school mobile technology policy and the law.

Online communication, including use of social media

27. 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 and Safeguarding, code of conduct, social media policy and the law.
28. As outlined in the staff code of conduct and school social media policy:
- I will take appropriate steps to protect myself and my reputation, and the reputation of the school, online when using communication technology, including the use of social media.
 - I will not discuss or share data or information relating to children, staff, school business or parents/carers on social media.

29. My electronic communications with current and past children and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
- I will ensure that all electronic communications take place in a professional manner via school approved and provided communication channels and systems, such as a school email address, user account or telephone number.
 - I will not share any personal contact information or details with children, such as my personal email address or phone number.
 - I will not add or accept friend requests or communications on personal social media with current or past children and their parents/carers.
 - If I am approached online by a current or past child or parents/carers, I will not respond and will report the communication to my line manager and (Mrs E Pearson) Designated Safeguarding Lead (DSL).
 - Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL and/or headteacher.

Policy concerns

30. 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.
31. 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.
32. 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.
33. I will report and record any concerns about the welfare, safety or behaviour of children or parents/carers online to the DSL in line with the school's child protection policy.
34. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, or SLT in line with school child protection policy.

Policy Compliance and Breaches

35. 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 DSLs and the headteacher.
36. 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.

- 37. 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.
- 38. I understand that if the school believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the staff code of conduct.
- 39. 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 Teynham CE Primary School'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).....

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 Teynham CE Primary School 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, either provided to me by the school or accessed by me as part of my role within Teynham CE 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 Teynham CE Primary School AUP should be read and followed in line with the school staff code of conduct.
3. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the school ethos, school staff code of conduct and safeguarding policies, national and local education and child protection guidance, and the law.
4. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.
5. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.
6. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

Data and image use

7. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including UK GDPR.
8. I understand that I am not allowed to take images or videos of children. Any images or videos of children will only be taken in line with the school camera and photograph policy.

Classroom practice

9. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of children.
10. I will support and reinforce safe behaviour whenever technology is used on site, and I will promote online safety with the children in my care.
11. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the school community, I will report this to the DSL and IT provider, in line with the school child protection policy.
12. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

Use of mobile devices and smart technology

13. In line with the school mobile and smart technology policy, I understand that my personal device must be switched off or on silent mode when inside the school building.

Online communication, including the use of social media

14. I will ensure that my online reputation and use of technology and is compatible with my role within the school. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
 - I will take appropriate steps to protect myself online as outlined in the child protection and social media policy (website)
 - I will not discuss or share data or information relating to children, staff, or school business or parents/carers on social media.
 - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the school code of conduct and the law.
15. My electronic communications with children, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
 - All communication will take place via school approved communication channels such as via a school provided email address, account or telephone number.
 - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
 - Any pre-existing relationships or situations that may compromise my ability to comply with this will be discussed with the DSL or headteacher.

Policy compliance, breaches or concerns

- 16. If I have any queries or questions regarding safe and professional practice online either in school or off site, I will raise them with the Designated Safeguarding Lead (Mrs E Pearson) headteacher.
- 17. I understand that the school may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of children and staff. This includes monitoring all school provided devices and school systems and networks including school provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
- 18. I will report and record concerns about the welfare, safety or behaviour of children or parents/carers online to the Designated Safeguarding Lead (Mrs E Pearson) in line with the school child protection policy.
- 19. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with the allegations against staff policy.
- 20. 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.
- 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 Teynham CE 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

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school boundaries and requirements when using the school Wi-Fi systems and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

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

1. The school provides Wi-Fi for the school community and allows access for education or related business use only.
2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the school premises that is not the property of the school.
3. The use of technology falls under Teynham CE Primary School Acceptable Use of Technology Policy (AUP), and Code of Conduct which all children/staff/visitors and volunteers must agree to and comply with.
4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.
5. School owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
6. I will take all practical steps necessary to make sure that any equipment connected to the school service is adequately secure, such as up-to-date anti-virus software, systems updates.
7. The school wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.
8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.
10. I will not attempt to bypass any of the school security and filtering systems or download any unauthorised software or applications.
11. My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.
13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Mrs E Pearson) as soon as possible.
14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (Mrs E Pearson) 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 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 Teynham CE Primary School Wi-Fi Acceptable Use Policy.

Name

Signed:Date (DDMMYY).....

Acceptable Use Policy (AUP) for Remote/Online Learning

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

- LGfL: [Safeguarding Considerations for Remote Learning](#)

- SWGfL: [Which Video Conference platform is best?](#)

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

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

Remote/Online Learning AUP

Teynham CE Primary School Staff Remote/Online Learning AUP

The Remote/Online Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of school community when taking part in remote/online learning, for example following any full or partial school closures.

Leadership oversight and approval

1. Remote/online learning will only take place using Zoom or Teams.
 - These has been assessed and approved by the headteacher.
2. Staff will only use school managed or specific, approved professional accounts with children and parents/carers.
 - Use of any personal accounts to communicate with children and parents/carers is not permitted.
 - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with Mrs E Pearson, Designated Safeguarding Lead (DSL).
 - Staff will use work provided equipment where possible, for example, a school/setting laptop or ipad.
3. Online contact with children and parents/carers will not take place outside of the operating times as defined by SLT:
 - 9am-3.20pm
4. All remote/online lessons will be formally timetabled; a member of SLT or DSL is able to drop in at any time.

5. Live-streamed remote/online learning sessions will only be held with approval and agreement from the headteacher or member of SLT.

Data Protection and Security

6. Any personal data used by staff and captured by the system when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection/GDPR policy (website).
7. All remote/online learning and any other online communication will take place in line with current school confidentiality expectations as outlined in Code of Conduct policy, Mobile, Smart Technology and Social Media policy
8. Only members of the Teynham CE Primary School community will be given access to Teams or Zoom.
9. Access to Teams or Zoom will be managed in line with current IT security expectations as outlined in Staff AUP.

Session management

10. Staff will record the length, time, date, and attendance of any sessions held.
11. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
 - Waiting rooms
 - Muting children on entry
12. When live streaming with children:
 - contact will be made via the provided logins.
 - contact will be made via a parents/carers account.
 - staff will mute children's videos and microphones.
 - at least 2 members of staff will be present.
 - If this is not possible, SLT approval will be sought.
13. Live 1:1 sessions will only take place with approval from the a member of SLT.

14. A pre-agreed email detailing the session expectations will be sent to those invited to attend.
- Access links should not be made public or shared by participants.
 - Children and parents/carers should not forward or share access links.
 - If children or parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
 - Children are encouraged to attend lessons in a shared space or room with an open door and when appropriately supervised by a parent/carer or another appropriate adult.
15. Alternative approaches and access will be provided to those who do not have access. The school can provide a number of devices to loan to children.

Behaviour expectations

16. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
17. All participants are expected to behave in line with existing school policies and expectations. This includes:
- Appropriate language will be used by all attendees, including parents.
 - Staff will not take or record images for their own personal use.
18. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
19. When sharing videos and/or live streaming, participants are required to:
- wear appropriate dress.
 - ensure backgrounds of videos are neutral (blurred if possible).
 - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
20. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

21. Participants are encouraged to report concerns during remote and live-streamed sessions:
- Tell a parent or carer
 - Report to the adult running the session
22. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to SLT and parents/carers.

- 23. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.
- 24. Sanctions for deliberate misuse may include, restricting use, removing the child from the session or reporting to the Police if a crime has been committed.
- 25. Any safeguarding concerns will be reported to Mrs E Pearson, Designated Safeguarding Lead, in line with our child protection policy.

<p>I have read and understood the Teynham CE Primary School Acceptable Use Policy (AUP) for remote/online learning.</p> <p>Staff Member Name:</p> <p>Date.....</p>

Acknowledgements and Thanks

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

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