KENT LADO EDUCATION SAFEGUARDING ADVISORY SERVICE

Acceptable Use of Technology Policy

In line with The Education People Acceptable Use of Technology Policy Template for Educational Settings (August 2025)

Written by	V Levy
Approved by	Resources Committee
Date Created	November 2023
Latest Review	October 2025
Latest Approval Date	24th November 2025
Version	3

Contents

Acceptable Use of Technology Policy – Learner Agreement - Early Years and Key Stage 1 (0-6) 3
Acceptable Use of Technology Policy – Learner Agreement - Key Stage 2 (7-11) 4
Acceptable Use of Technology Policy – Parent / Carer Acknowledgement Form 9
Acceptable Use of Technology Policy (AUP) – Parent / Carer Agreement 11
Acceptable Use of Technology Policy for Staff, Visitors and Volunteers 14
Acceptable Use of Technology Policy – Visitor / Volunteer Agreement 21
Wi-Fi Acceptable Use Policy 24
Acceptable Use of Technology – Remote Learning and Online Communication for Staff 26
Acceptable Use of Technology – Remote Learning for Learners 29

Acceptable Use of Technology Policy – Learner Agreement - Early Years and Key Stage 1 (0-6)

- I understand that the Higham Primary School Acceptable Use Policy will help keep me safe and happy when I go online.
- I only go online when an adult is with me.
- I only click on online things when I know what they do. If I am not sure, I ask an adult first.
- I keep my personal information and passwords safe.
- I only send polite and friendly messages online.
- I know that Higham Primary School can see what I am doing online when I use school ipads, desktop computers or other school systems and any online web-based programmes including if I use them at home.
- If I see something online that makes me feel upset, unhappy, or worried I will always tell an adult.
- I can visit www.ceopeducation.co.uk to learn more about keeping safe online.
- I know that if I do not follow the rules an adult will speak to me and consequences will be as per the traffic light systems and my parents may be contacted.
- I have read and talked about these rules with my parents/carers.

Shortened KS1 version (e.g. for use on posters)

- 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

Acceptable Use of Technology Policy – Learner Agreement - Key Stage 2 (7-11)

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

Safe

- I will be kind and respectful online, just like I am in school.
- I will only send messages which are polite and friendly. When I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.
- I will only share pictures or videos online if they are safe, kind, and I have asked for permission first.
- I only talk with and open messages from people I know.
- I will only click on links if a trusted adult says they are safe.
- I know that people online might not be who they say they are. I will only chat with people I know or who a trusted adult says are safe.
- I will protect myself by not telling anyone I meet online my address, my telephone number, my age, my school name or by sending a picture of myself without permission from a teacher or other adult.
- If I get unpleasant, rude, or bullying emails or messages, I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- If someone online asks to meet me, I will tell a trusted adult straight away.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.

Learning

- I know that I will be able to use the internet in school for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to the use internet or computers/ipads at school.
- I ask my teacher before using my own personal smart devices and/or mobile phone at school.
- I always ask permission from an adult before using the internet.
- I only use websites, tools and/or search engines that my teacher has chosen or given me permission to use..
- I use school devices 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 some things or people online might not be honest or truthful.
- If I'm not sure something online is true, I will check with other websites, books, or ask a trusted adult.
- I always credit the person or source that created any work, images, or text I use.

- I will always check before I download software or data from the internet. I know that information on the internet may not be reliable and it sometimes needs checking.
- If I bring in portable media and/or removable storage from outside of school, I will always give them to my teacher so they can be checked for viruses and content before opening them.
- I will use Artificial Intelligence (AI) tools safely and sensibly. I won't use them to cheat, copy other people's work, or say anything unkind. I know that AI tools can sometimes make mistakes. I will only use them when a teacher or trusted adult says it's okay.

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.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these I should report it to a teacher or adult in school, or a parent or carer at home.

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 or put the iPad face down and tell an adult immediately.
- If I am aware of anyone being unsafe with technology, I will report it to an adult at Higham Primary School.
- I know it is not my fault if I see, or someone sends me, something upsetting or unkind online.
- If I'm not sure about something online or it makes me feel worried or scared, I will talk to a trusted adult.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all school owned devices and networks are checked/monitored to help keep me safe, even if I use them at home. This means someone at Higham Primary School may be able to see and/or check my online activity when I use school devices and/or networks if they are worried 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 know that it is to be handed in to the school office and then collected at the end of the school day.
- I have read and talked about these rules with my parents/carers.
- I know that I am not allowed on personal email, social networking sites or instant messaging in school.
- I can visit www.ceopeducation.co.uk and www.childline.org.uk to learn more about being safe online.

- I know that if I do not follow the rules an adult will speak to me and consequences will be as per the traffic light systems and my parents may be contacted. At the discretion of the headteacher, I may no longer be allowed access to the internet or use the computers or iPads in school.

Shortened KS2 version (for use on posters)

- I ask a teacher 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.
- I trust and visit www.ceopeducation.co.uk
- I will use Artificial Intelligence (AI) tools safely and sensibly. I will only use them when a teacher or trusted adult says it's okay.

Acceptable Use of Technology Policy – Learner Agreement Form (Key Stage 2 as appropriate)

Higham Primary School Acceptable Use of Technology Policy – Learner Agreement

I, with my parents/carers, have read and understood the Higham Primary School Acceptable Use of Technology Policy (AUP) and remote learning AUP

I agree to follow the AUP when:

1. I use school devices and systems, both on site and at home.
2. I use my own devices in school when allowed, including mobile phones, smart technology gaming devices, and cameras.
3. I use my own equipment out of the school, including communicating with other members of the school or when accessing school systems.

Child's Name…… Signed…….

Class …… Date ……

Parent/Carers Name……..

Parent/Carers Signature…… Date ……..

Acceptable Use of Technology Policy – Parent / Carer Acknowledgement Form

I, with my child, have read and discussed Higham Primary School Acceptable Use of Technology Policy (AUP) – Learner Agreement and understand that the AUP will help keep my child safe online.

1. I understand that the AUP applies to my child use of school devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another pupil, could have repercussion for the orderly running of the school, if a pupil is identifiable as a member of the school, or if behaviour could adversely affect the reputation of the school.

2. I understand that any use of school devices and systems are appropriately filtered; this includes the Netsweeper Filtering and Monitoring' system.

3. I am aware that any use of school devices and systems may be monitored for safety and security reasons, when used on and off site. this includes the 'Netsweeper Filtering and Monitoring' system. 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 (including GDPR), privacy, and human rights legislation.

4. 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.

5. 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. Learners' personal devices and mobile phones are to be handed into the school office each morning and are returned at the end of the day.

6. 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's remote learning AUP. When accessing video learning, I will ensure they are an appropriate location (e.g. not in bed) and that they are suitably dressed.

7. 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.

8. 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.

9. I will inform the school (for example speak to a member of staff and/or the Designated Safeguarding Lead or deputies in their absence) or other relevant organisations if I have concerns over my child's or other members of the school communities' safety online.

10. 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.

11. I understand my role and responsibility in supporting the school 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.

Acceptable Use of Technology Policy – Parent / Carer Acknowledgement Form

Higham Primary School Acceptable Use of Technology Policy – Parent Acknowledgement Form

I have read and understood the Higham Primary School Acceptable Use of Technology Policy (AUP) and Ackowledgement Form

Child's Name……. Date…….

Parent/Carers Name……

Acceptable Use of Technology Policy (AUP) – Parent / Carer Agreement

1. I know that my child will be provided with internet access and will use a range of IT systems in order to access the curriculum and be prepared for modern life whilst at Higham Primary School.

2. I understand that the AUP applies to my child's use of Higham Primary School devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another pupil, could have repercussions for the orderly running of the school, if a pupil is identifiable as a member of the school, or is the behaviour could adversely affect the reputation of the school.

3. I am aware that use of mobile and smart technology, such as mobile phones or smart watches by children is not permitted at Higham Primary School.

4. I understand that any use of school devices and systems are appropriately filtered. We currently use Netsweeper for our filtering and monitoring.

5. I am aware that my child's use of school provided device and systems will be monitored for safety and security reasons, when used on and offsite with our Netsweeper monitoring and filtering system. 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.

6. 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.

7. I am aware 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.

8. I have read and discuss Higham Primary Schools Pupil Acceptable Use of Technology Policy (AUP) with my child.

9. I will support school safeguarding policies and will ensure that I use appropriate parental controls, will appropriately monitor my child's use of the internet outside of school and discuss online safety with them when they access technology at home.

10. I know I can seek support from the school about online safety, such as via the school website, to help keep my child safe online at home.

11. I will support the school approach to online safety. I will role model safe and positive online behaviour for my child by sharing images, text, and video online responsibly.

12. I, together with my child, 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.

13. I understand that a partnership approach to online safety is required. If the school has any concerns about either my of my child's behaviour or safety online, then I will be contacted.

14. I understand that if I or my child do not abide by the Higham Primary School AUP, appropriate action will be taken. This could include sanctions beings applied in line with the school behaviour policy and if a criminal offence has been committed, the police being contacted.

15. I know that I can speak to the Designated Safeguarding Lead (C Grattan) or deputy DSL's (V Levy, C Driscoll, A Dunn) in her absence, my child's teacher or the headteacher if I have concerns about online safety.

16. At Higham Primary School we cannot dictate to you as parents/carers the social media/gaming platforms that you allow your child to use. As a parent I will make myself aware of age guidance on Facebook, Whatsapp, TikTok, Twitter, Instagram, gaming platforms and any other forms of social media platforms and I will use my parental responsibility to keep my child safe. (As a school we have found that use of these platforms can spill over into class interaction and sometimes cause upset).

Acceptable Use of Technology Policy – Parent / Carer Agreement Form

Higham Primary School Acceptable Use of Technology Policy – Parent Agreement

I have read, understood and agree to comply with the Higham Primary School Acceptable Use of Technology Policy (AUP)

Child's Name…… Date…….

Parent/Carers Name……

Acceptable Use of Technology Policy for Staff, Visitors and Volunteers

Acceptable Use of Technology Policy – Staff Agreement

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Higham 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 learners, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

At Higham Primary School we will only use age appropriate learning and learning will be adapted according to a child/class age and needs.

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 Higham Primary School'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 Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school or accessed as part of my role within Higham Primary School both professionally and personally, both on and offsite. This may include my use of 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 Higham Primary School's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school Code of Conduct for staff and volunteers and remote learning AUP.

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 Higham Primary School Devices and Systems

4. When working with learners, I will only use the equipment and internet services provided to me by Higham Primary School for example school provided laptops, tablets, mobile phones, and internet access. However, my personal mobile phone may be used when required for multi-factor authentication purposes.

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, occasional personal use of school IT systems and/or devices by staff is allowed to support work-life balance and the development of staff IT skills. However, this is 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. Passwords should be changed regularly and at least annually.
    - I will protect the devices in my care from unapproved access or theft. Laptops and school iPads must not be left unattended in the car, overnight or for long periods of time. (See Confidentiality Policy)
    - I am responsible for information stored on laptops and iPads and I will take the necessary measures to do all I can to keep that information safe.
    - I will use multi-factor authentication where possible

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

9. I will not allow unauthorised individuals to access email / internet / intranet / network / social networks / mobile apps / or any other system I have access to via the school or school umbrella.

10. 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 technician.

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

12. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK GDPR in line with the school GDPR and Data Protection Policy and Confidentiality Policy.
    - 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.
    - portable media and/or removable storage Any data being removed from the school site, such as via email or portable media and/or removable storage, 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.

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

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

15. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

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

17. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the IT Technician (S Walton) as soon as possible.

18. If I have lost any school related documents or files, I will report this to the IT Technician (S Walton) and school Data Protection Officer (Satswana) discussions soon as possible.

19. Any images or videos of learners, devices and portable media and/or removable storage, will only be used as stated in the schools Image Use Policy.

Classroom Practice

20. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by Higham Primary School as detailed in child protection policy, mobile and smart technology policy and social media policy, and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.

21. If there is a 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 Technician, in line with the school's child protection policy, mobile and smart technology policy and social media policy.

22. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in child protection policy, mobile and smart technology policy, social media policy and remote learning AUP.

23. 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:

- AI tools are only to be used responsibly and ethically, and in line with our child protection, data protection and code of conduct policy expectations
- I am required to critically evaluate any AI-generated content for accuracy, bias, and appropriateness before sharing or using it in educational contexts.
- AI must not be used to replace professional judgement, especially in safeguarding, assessment or decision-making involving pupils.
- Only approved AI platforms may be used with pupils. Pupils must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
- Any misuse of AI will be responded to in line with relevant school/college policies, including but not limited to, anti-bullying, staff and pupil/student behaviour and child protection.
- AI tools will not be used in situations that involve the processing of personal, sensitive, or confidential information.

24. I have read and understood the school mobile and smart technology policy and social media policy.

25. I will promote online safety with the learners 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 learners 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) or a deputy as part of planning online safety lessons or activities to ensure support is in place for any learners 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 learners is appropriate.

26. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

Mobile devices and smart technology

27. I have read and understood the school mobile and smart technology and social media policies which addresses use by pupils and staff.

28. 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's mobile and smart technology and social media policy and the law.

Online communication, including use of social media

29. 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, staff code of conduct policy, mobile and smart technology and social media policy and the law.

30. As outlined in the staff code of conduct and the school's 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 learners, 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.

31. My electronic communications with current and past learners 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 and systems, such as a school email address, user account or telephone number.
    - I will not share any personal contact information or details with learners, 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 learners and/or parents/carers, unless by prior arrangement through discussion with the headteacher.
    - If I am approached online by a learner or parents/carer, I will not respond and will report the communication (C Grattan) 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

32. 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.

33. 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.

34. 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.

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

36. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with the school's child protection policy and Whistleblowing Policy.

Policy Compliance and Breaches

37. 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.

38. 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 pace in accordance with data protection, privacy, and human rights legislation.

39. 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 code of conduct.

40. 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 code of conduct.

41. 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 Higham 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)……

Acceptable Use of Technology Policy – Visitor / Volunteer Agreement

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 our behaviour expectation and their professional responsibilities when using technology.

This AUP will help Higham 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 Higham Primary School both 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 Higham Primary School AUP should be read and followed in line with the school code of conduct for staff and volunteers

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 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 materials, adult pornography covered by the Obscene Publication 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 learners without prior agreement of the headteacher. Any images or videos of learners will only be taken in line with the school photographic image 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 learners.

10. Where I deliver or support remote learning, I will comply with the school remote learning AUP.

11. I will support staff in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the children in my care.

12. I will immediately report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) (C Grattan) in line with the school child protection policy.

13. 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 Technician, in line with the school child protection and mobile and smart technology and social media policy.

14. 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

15. In line with the school's mobile and smart technology and social media policy, I understand the expectations regarding visitor use of social media and mobile technology.

Online communication, including the use of social media

16. 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 mobile and smart technology and social media policy.
    - I will not discuss or share data or information relating to learners, staff, 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.

17. My electronic communications with learners, 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 (C Grattan) and/or headteacher.

Policy compliance, breaches or concerns

18. 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 (C Grattan) and/or the headteacher.

19. 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.

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

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

22. 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.

23. I understand that if the school suspects criminal offences have occurred, the police will be informed.

24. 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.

25. 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.

26. 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.

I have read, understood and agreed to comply with Higham 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 use only during the school day, but team members can access the Wi-Fi before school, at breaktimes, at lunchtimes and after school when no child is present.

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 Higham Primary School Acceptable Use of Technology Policy (AUP), child protection policy, mobile and smart technology and social media policy, GDPR & Data Protection policy and behaviour policy which all learners/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 (C Grattan) as soon as possible.

14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (C Grattan) 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 Higham Primary School Wi-Fi Acceptable Use Policy.

Name ……..

Signed: ……Date (DDMMYY)……

Acceptable Use of Technology – Remote Learning and Online Communication for Staff

The Remote Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of the Higham Primary School community when taking part in remote learning following any full or partial school closures.

Leadership Oversight and Approval

1. Remote learning will only take place using Microsoft TEAMS, Google Classroom or Tapestry.
   - Microsoft Teams, Google Classroom and Tapestry has been assessed and approved by the headteacher and members of Senior Leadership Team (SLT).

2. Staff will only use school managed or specific, approved professional accounts with learners and/or parents/carers.
   - Use of any personal accounts to communicate with learners and/or parents/carers is not permitted. Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with C Grattan, Designated Safeguarding Lead (DSL).
   - Staff will use work provided equipment where possible e.g. a school laptop, tablet, or other mobile device.

3. Online contact with learners and/or parents/carers will not take place outside of the working week and will only take place between 8.30am and 5.00pm.

4. All remote lessons will be formally timetabled; a member of SLT or a DSL is able to drop in at any time.

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

Data Protection and Security

6. Any personal data used by staff and captured by Microsoft TEAMS or Tapestry when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.

7. All remote learning and any other online communication will take place in line with current school confidentiality expectations as outlined in the Remote Learning policy.

8. All participants will be made aware that to Microsoft TEAMS, Google Classroom and Tapestry records activity.

9. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements.

10. Only members of the Higham Primary School community will be given access to Microsoft TEAMS, Google Classroom and Tapestry.

11. Access to Microsoft TEAMS, Google Classroom and Tapestry will be managed in line with current IT security expectations as outlined in the Remote Learning policy.

Session Management

12. Staff will record the length, time, date, and attendance of any sessions held.

13. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
    - disabling/limiting chat, staff not permitting learners to share screens, staff muting learners at any time, signing into meetings as themselves, camera's being on, keeping meeting IDs private and use of waiting rooms/lobbies.

14. When live streaming with learners:

    - contact will be made via learners' school provided email accounts and/or TEAMS logins.
    - contact will be made via a parents/carer account.
    - staff will mute/disable learners' videos and microphones if required.
    - at least 2 members of staff will be present. If this is not possible, SLT approval will be sought.

15 Live 1 to 1 sessions will only take place with approval from the headteacher/a member of SLT. A parent/carer must be present in the room for these sessions. If a parent/carer is not present the session will be ended and school will contact parent.

16 A pre-session agreement is sent to all parent stating session expectations:
- Access links should not be made public or shared by participants.
- Learners and/or parents/carers should not forward or share access links.
- If learners/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
- Learners are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.

17 Alternative approaches and/or access will be provided to those who do not have access. E.g the loan of school equipment to those who are eligible and as required.

Behaviour Expectations

18 Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.

19 All participants are expected to behave in line with existing school policies and expectations. This includes:
- Appropriate language will be used by all attendees.
- Staff will not take or record images for their own personal use.

20 Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.

21 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.

22 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

23 Participants are encouraged to report concerns during remote and/or live streamed sessions:

24 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 the headteacher.

25 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.

26 Sanctions for deliberate misuse may include: restricting/removing use, informing parents/carers, contacting police if a criminal offence has been committed.

27 Any safeguarding concerns will be reported to C Grattan, Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the Higham Primary School Acceptable Use Policy (AUP) for Remote Learning and Online Communication for Staff.

Staff Member Name: ……

Date……

Acceptable Use of Technology – Remote Learning for Learners

1 I understand that:
- These expectations are in place to help keep me safe when I am learning at home using Microsoft Teams, Google Classroom or Tapestry.
- I should read and talk about these rules with my parents/carers.
- Remote learning will only take place using Microsoft TEAMS, Google Classroom or Tapestry and during usual school times.
- My use of Microsoft TEAMS, Google Classroom or Tapestry is monitored to help keep me safe.

2. Only members of Higham Primary School community can access TEAMS, Google Classroom and Tapestry.
- I will only use my school provided email accounts and/or login to access remote learning.
- I will use privacy settings as agreed with my teacher and set up the school.
- I will not share my login/password with others
- I will not share any access links to remote learning sessions with others.

3. When taking part in remote learning I will behave as I would in the classroom as per the school rules. This includes:
- Using appropriate language.
- Treating others with respect.
- Not taking or recording images/content without agreement from the teacher and/or those featured.

4. When taking part in live sessions I will:
- Mute my microphone unless I am asked to respond.
- Wear appropriate clothing and be in a suitable location.
- Ensure backgrounds of videos are neutral and personal information/content is not visible.
- Use appropriate alternative backgrounds.
- Attend the session in full. If for any reason I cannot attend a session in full, I will let my teacher know.
- Attend lessons in a shared/communal space or room with an open door and/or where possible when I can be supervised by a parent/carer or another appropriate adult.

5. If I am concerned about anything that takes place during remote learning, I will tell the member of staff running the session and/or tell a parent/carer.:

6. I understand that inappropriate online behaviour or concerns about my safety during remote learning will be taken seriously. This could include:
- restricting/removing access, informing parents/carers, contacting police if a criminal offence has been committed.

I have read and understood the Higham Primary School Acceptable Use Policy (AUP) for remote learning.

Pupil's Name……

Signed…… Date……

Parent/Carers Name……