E-Safety and Acceptable Use Policy

Version number: V1

Date adopted by Local Governing Body: May 26

Scheduled review date: May 27

Statutory or Best Practice policy: Best Practice

Meeting your communication needs:

We want to ensure that your needs are met. If you would like this information in any other format, please contact us on 01637 880272 or email scmajor@kernowlearning.co.uk

E-Safety and Acceptable Use of Technology Policy

Contents

Contents 1
1. Introduction 2
2. Responsibilities 2
3. Scope of policy 2
4. Policy and procedure 3
   Use of email 3
   Visiting online sites and downloading 3
   Storage of Images 4
   New technological devices 5
   Reporting incidents, abuse and inappropriate material 5
5. Curriculum 5
6. Staff and Governor Training 6
7. Working in Partnership with Parents/Carers 6
8. Records, monitoring and review 6

Guidance Notes ..... **Error! Bookmark not defined.**

Appendix 1 - Pupil Acceptable Use of Technology Sample Statements 8
Appendix 2 - Pupil Acceptable Use Policy Agreement Form 10
Appendix 3 - Acceptable Use of Technology Sample Statements and Forms for Families 11
Appendix 4 - Family Acceptable Use of Technology Policy 13
Appendix 5 - Acceptable Use of Technology for Staff, Visitors and Volunteers 15
Appendix 6 - Visitor and Volunteer Acceptable Use of Technology Policy 19

1. Introduction

Kernow Learning recognises that internet, mobile and digital technologies provide positive opportunities for children to learn, socialise and play but that our pupils also need to understand the challenges and risks associated with the technology. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all pupils, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

Kernow Learning is also committed to ensuring that all those who work with children and young people, including their families, are informed about the ever-changing risks so that they can take an active part in helping children to navigate the online world safely and confidently.

2. Responsibilities

The headteacher has ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety lead in this school is Tracey Milsom

All breaches of this policy must be reported to the headteacher or online safety Lead Tracey Milsom

All breaches of this policy that may have put a child at risk must also be reported to the lead DSL.

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount, and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

3. Scope of policy

The policy applies to:

- pupils
- families of pupils
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for families, for example, through the website, in newsletters and at events. It is important that family members understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe in Education, health and safety, remote learning, behaviour, and anti-bullying.

4. Policy and procedure

The school seeks to ensure that internet, digital, mobile and smart technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, smart, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, families, staff and governors and all other visitors to the school.

Use of email

Staff and governors should use a Kernow Learning allocated email account for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils should use school approved accounts on the school system for educational purposes. Where required parent/carer permission will be obtained for the pupil account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to the Chief Operating Officer, this may be via your class teacher or headteacher.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a Kernow Learning senior leader. The terms and conditions of the service should be read and adhered to, and families permission sought where required. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.

Staff must only use pre-approved systems if creating blogs, wikis or other online content.

When working with pupils searching for images should be done through Google Safe Search or a similar application that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)

- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten, or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

Only a school device may be used to conduct school business outside of school. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device. Such a system would ensure the user was not saving files locally to their own device and breaching data security.

Our Trust and school acknowledges the growing presence of AI technologies. To ensure the responsible and secure use of such tools, this policy also applies to AI and the following guidelines have been established:

- **Confidentiality and Data Protection**: Staff must not input, upload, or share any confidential, sensitive, or personally identifiable information related to pupils, parents, staff, or the school community into AI platforms.
- **Evaluation and Approval**: Before integrating any AI tool into the classroom or administrative processes, staff are required to evaluate its suitability with the headteacher, who will liaise with our Trust Safeguarding Lead as needed.
- **Training and Awareness**: The school will provide training sessions and resources to ensure that all staff members are aware of the implications of using AI tools and are equipped to make informed decisions regarding their use.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of families which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by families at any time.

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud-based services. Rights of access to stored images are restricted to approved staff. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Families should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons families must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Families, pupils and staff should not assume that new technological devices will be allowed in school and should check with the headteacher before they are brought into school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSL, the headteacher or the Trust Safeguarding Lead. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

5. Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive age-appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies.

Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online behaviour and reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others

- Understanding the permanency of all online postings and conversations
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.
- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- Understanding of how technology continues to evolve
- How the law can help protect against online risks and abuse

6. Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies.

All staff and governors receive online safety training at the point of induction, which is renewed on an annual basis. Staff also receive separate filtering and monitoring training. This details the specific processes that we use across Kernow Learning and is delivered at the point of induction and renewed on an annual basis All training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation working with children and based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement.

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement.

Guidance is provided for occasional visitors, volunteers and family helpers.

7. Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of families is essential to implement the online safety policy effectively and help keep children safe.

It is important that families understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with families and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Families are asked on an annual basis to read, discuss and co-sign with each child the Acceptable Use Agreement. The Acceptable Use Agreement explains the school's expectations and pupil and family responsibilities.

8. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported, and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the

school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes.

Appendix 1 - Pupil Acceptable Use of Technology Sample Statements

Early Years and Key Stage 1

I understand that my 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 tablets and on PurpleMash Times table Rockstars, Busythings, Teams and Microsoft applications, including when I am at home.
- I always tell a Trusted Adult if something online makes me feel upset, unhappy, or worried.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
- I know that if I do not follow the rules:
    - Step 1 -I will receive a warning.
    - Step 2 I will have time out away from the device where I will talk about my actions with a Trusted Adult.
    - Step 3 I will receive a negative Dojo and my parents/carers will be contacted.
- I have read and talked about these rules with my parents/carers.

Key Stage 2

I understand that my 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 not bring any mobile phones into school. If there is an exceptional reason agreed by the headteacher it will be handed in to the office to be locked away for 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 unless I have permission otherwise.
- If I need to learn online at home, I will follow the school remote learning policy.
- I will only save work/images when instructed to in my Teams area.

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.

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 devices and systems are monitored to help keep me safe, including when I use them at home.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online.
- I know that if I do not follow the school rules then:

-Step 1 -I will receive a warning.

-Step 2 I will have time out away from the device where I will talk about my actions with a Trusted Adult.

-Step 3 I will receive a negative Dojo and my parents/carers will be contacted.

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page or shut the laptop lid and tell an adult straight away.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher or Trusted Adult.
- I know it is not my fault if I see, or someone sends me, something bad online. I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.

Appendix 2 - Pupil Acceptable Use Policy Agreement Form

St Columb Major Academy Acceptable Use of Technology Policy – Pupil Agreement

I, with my family, have read and understood St Columb Major Academy's Acceptable Use of Technology Policy.

I agree to follow the Acceptable Use Policy when:

1. I use school devices and systems (PurpleMash Times table Rockstars, Busythings, Teams and Microsoft applications and those chosen by my teacher), both on site and at home.
2. I use my own equipment out of the school including communicating with other members of the school or when accessing school systems.

Name…… Signed……..…..

Class…… Date……

Parent/Carer's Name……..……..... (**If appropriate**)

Parent/Carer's Signature…… (**If appropriate**)

Date……

Appendix 3 - Acceptable Use of Technology Sample Statements and Forms for Families

St Columb Major Academy's Pupil Acceptable Use of Technology Policy Acknowledgment

1. I have read and discussed St Columb Major Academy's pupil acceptable use of technology policy with my child and understand that the AUP will help keep my child safe online.

2. I understand that this applies to my child's use of school devices and systems on site and at home including (iPads, Laptops, PurpleMash Times table Rockstars, Busythings, Teams and Microsoft applications and those chosen by the class teacher), 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 if the behaviour could adversely affect the reputation of the school.

3. I am aware that any use of school devices and systems are appropriately filtered and may be monitored for safety and security reason 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. All Kernow Learning schools use a system called SENSO to filter and monitor online use.

   I am aware that
   - The school will only agree to a pupil bringing a mobile phone to school if they travel to and from school without adult supervision as an exceptional circumstance.
   - When a child needs to bring a phone into school for an exceptional circumstance, the phone must be left in the school office at the start of the day and collected at the end of the day. Phones should be clearly marked so that each pupil can identify their own phone. Parents are advised that the school accept no liability for the loss or damage to mobile phones which are brought into school or school grounds.
   - If a pupil is found taking photographs, video footage or audio recordings with a mobile phone of either other pupils or teachers, this will be regarded as a serious offence and action will be taken according to our Behaviour Policy.
   - We ask that parents should talk to their children about the appropriate use of text messages and social media. Should parents need to contact pupils or vice versa during the school day, this should be done via the usual school procedure of contacting the school office via phone or email.
   - The use of mobile phones by pupils is supported by Behaviour, Safeguarding and E-Safety Policies of the school.
   - Pupils must adhere to the school's Acceptable Use Agreement.

4. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed online or if my child is using personal mobile or smart technologies.

5. 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.

6. 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.

7. I will inform the school if I have concerns over my child's or other members of the school community's safety online.

8. 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.

9. 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.

Child's Name…… Child's Signature …….... (***if appropriate***)

Class……..…… Date……..……

Parent/Carer's Name…….....

Parent/Carer's Signature…….... Date…….

Appendix 4 - Family Acceptable Use of Technology Policy

1. I know that my child will be provided with internet access and will use a range of IT systems including iPads, Laptops, PurpleMash Times table Rockstars, Busythings, Teams and Microsoft applications and those chosen by the class teacher in order to access the curriculum and be prepared for modern life whilst at this school.
2. I understand that the Acceptable Use Policy applies to my child's use of school devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another pupil, could have repercussions for the orderly running of the school, if a pupil is identifiable as a member of the school/setting, or if the behaviour could adversely affect the reputation of the school/setting.
3. I am aware that use of mobile and smart technology, such as mobile phones by children, has rules which need to be adhered to:
    - Only in exceptional circumstances, if agreed by the headteacher, a child can bring a mobile phone to school.
    - When a child has an exceptional reason for bringing a phone to school it must be left in the school office at the start of the day and collected at the end of the day. Phones should be clearly marked so that each pupil can identify their own phone. Parents are advised that the school accept no liability for the loss or damage to mobile phones which are brought into school or school grounds.
    - If a pupil is found taking photographs, video footage or audio recordings with a mobile phone of either other pupils or teachers, this will be regarded as a serious offence and action will be taken according to our Behaviour Policy.
    - If images or recordings of other pupils or adults have been taken, the phone will not be returned to the pupil until the material has been removed. Should a pupil be found to be using their phone inappropriately, the school reserves the right to withdraw this privilege and they will no longer be able to bring a phone into school.
    - We ask that parents should talk to their children about the appropriate use of text messages and social media. Should parents need to contact pupils or vice versa during the school day, this should be done via the usual school procedure of contacting the school office via phone or email.
    - The use of mobile phones by pupils is supported by Behaviour, Safeguarding and E-Safety Policies of the school.
    - Pupils must adhere to the school's Acceptable Use Agreement.

4. I am aware that any use of school devices and systems are appropriately filtered and may be monitored for safety and security reason 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. All Kernow Learning schools use a system called SENSO to filter and monitor online use.
5. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed online or if my child is using personal mobile or smart technologies.
6. 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.
7. I have read and discussed the pupil Acceptable Use of Technology Policy with my child.
8. I will support the school safeguarding policies and will ensure that I use appropriate parental controls, will appropriately supervise/monitor my child's use of the internet outside of school and will discuss online safety with them when they access technology at home.

9. 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.
10. 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.
11. 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.
12. I understand that a partnership approach to online safety is required. If the school has any concerns about either my or my child's behaviour or safety online, then I will be contacted.
13. I understand that if I or my child do not abide by the Acceptable Use of Technology Policy, appropriate action will be taken. This could include sanctions being applied in line with the school behaviour policy and if a criminal offence has been committed, the police being contacted.
14. I know that I can speak to the school if I have any concerns about online safety.

I have read, understood and agree to comply with the Families Acceptable Use of Technology Policy.

Parent/Carer's Name……

Parent/Carer's Signature…….. Date…….

Appendix 5 - Acceptable Use of Technology for Staff, Visitors and Volunteers

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

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the Acceptable Use Policy will help ensure that all staff understand our expectations regarding safe and responsible technology use and can manage the potential risks posed. The Acceptable Use Policy will also help to ensure that our 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 Policy applies to my use of technology systems and services provided to me or accessed as part of my role within school both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies.

2. I understand that our Acceptable Use of Technology Policy should be read and followed in line with our safeguarding policy and staff code of conduct

3. I am aware that this Acceptable Use Policy does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school's ethos 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 pupils.

5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed.

Data and system security

6. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
    - I will use a 'strong' password to access school systems.
    - I will protect the devices in my care from unapproved access or theft.
7. I will respect school system security and will not disclose my password or security information to others.

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

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

10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the Trust Data Protection 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.
    - 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.

11. 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.

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

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

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

15. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the Chief Operating Officer as soon as possible.

16. If I have lost any school related documents or files, I will report this to the Data Protection Officer as soon as possible.

17. I understand images of pupils must always be appropriate and should only be taken with school provided equipment and only be taken/published where pupils and/or parent/carers have given explicit written consent.

Classroom practice

18. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces.

19. I have read and understood the school mobile phone and social media policies.

20. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.

- creating a safe environment where pupils feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
- involving the E-Safety Lead when planning online safety lessons or activities to ensure support is in place for any pupils who may be impacted by the content.
- make informed decisions to ensure any online safety resources used with pupils is appropriate.

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

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

Mobile devices and smart technology

23. 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 Mobile Phone Policy and the law.

Online communication, including use of social media

24. 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 Safeguarding Policy, Staff Code of Conduct and the law.

25. 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 and I will not discuss or share data or information relating to pupils, staff, business or families on social media.

26. My electronic communications with current and past pupils and families 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 pupils, such as my personal email address or phone number.
    - I will not add or accept friend requests or communications on personal social media with current or past pupils and/or their families.
    - If I am approached online by a current or past pupil or their families, I will not respond and will report the communication to my Headteacher.
    - Any pre-existing relationships or situations that compromise my ability to comply with the Acceptable Use Policy or other relevant policies will be discussed with the DSL and/or headteacher.

Policy concerns

27. 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.

28. 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.

29. 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.

30. I will report and record any concerns about the welfare, safety or behaviour of pupils or their parents/carers online to the DSL in line with the school Safeguarding Policy.

31. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with the school Safeguarding Policy or Whistleblowing Policy.

Policy Compliance and Breaches

32. 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 or the headteacher.

33. I understand that the school may exercise its right to monitor the use of its information systems, including internet access and the interception of messages/emails on our systems, to monitor policy compliance and to ensure the safety of pupils and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

34. I understand that if the school believe that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the staff code of conduct.

35. 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.

36. 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 the 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)……

Appendix 6 - 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 St Columb Major Academy ensure that all visitors and volunteers understand the school expectations regarding safe and responsible technology use.

Policy scope

- I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services provided to me or accessed as part of my role within St Columb Major Academy both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning systems and communication technologies.

- I understand that St Columb Major Academy AUP should be read and followed in line with the school staff code of conduct.

- 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 St Columb Major Academy ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Data and image use

- I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.

Classroom practice

- I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of pupils.

    1. Using the internet to enhance learning as a planned part of the curriculum that will enrich and extend learning activities and is integrated into schemes of work. As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for Internet use.

    2. Different ways of accessing information from the Internet will be used depending upon the nature of the material being accessed and the age of the pupils:

    - access to the Internet may be by teacher demonstration
    - pupils may be given a suitable web site to access using a link from their year group links page on the school website or by clicking on a link in a teacher-prepared Word document
    - pupils may be provided with lists of relevant and suitable web sites which they may access
    - older pupils may be allowed to undertake their own Internet search having agreed a search plan with their teacher; pupils will be expected to observe the Rules of Responsible Internet

Use and will be informed that checks can and will be made on files and the sites they access.

- pupils accessing the Internet will be supervised by an adult, normally their teacher, at all times.

3. They will only be allowed to use the Internet once they have been taught the Rules of Responsible Internet Use (AUP) and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor the children using the Internet.

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

- I will immediately report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) (Marie Taylor) in line with the school child protection & online safety policy.

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

Use of mobile devices and smart technology

In line with the school mobile and smart technology policy, I understand that

- I will be asked to turn phones off when volunteering in classrooms.
- I will be asked to turn their phones to silent whilst attending assemblies and other pupil-based celebration events so that there is no disruption to the school's programs.
- Adults, either in school or accompanying children on school trips should not use their cameras or mobile phone cameras to take pictures or recordings of pupils.
- Adults, visitors or volunteers in school should only use their mobile phone or smart watch within the confines of the school office and personal cameras and mobile phone cameras should not be used to take pictures of children.

Online communication, including the use of social media

- 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 code of conduct.
  - I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.
  - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the school code of conduct/behaviour policy and the law.

- My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
  - All communication will take place via school approved communication channels such as via a school provided email address, account or telephone number.
  - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
  - Any pre-existing relationships or situations that may compromise my ability to comply with this will be discussed with the DSL (Marie Taylor).

Policy compliance, breaches or concerns

- 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 & Headteacher (Marie Taylor)
- 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.
- 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.
- 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 understand that the school may exercise its right to monitor the use of school information systems, including internet access and the interception of emails/messages on school systems, to monitor policy compliance and to ensure the safety pupils, staff and visitors/volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
- I will report and record concerns about the welfare, safety or behaviour of pupils or parents/carers online to the Designated Safeguarding Lead (Marie Taylor) in line with the school child protection policy.
- I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher in line with the allegations against staff policy.
- 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.
- 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 St Columb Major Academy's visitor/volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer: ……

Signed: ……

Date (DDMMYY)……