



St John's C of E Primary School

Online Safety and Acceptable Use of Technology Policy

School Policy	Summer 2026
School Staff were consulted on this document	Summer 2026
Adopted by the Full Governing Body	Summer 2026
To be reviewed	Autumn 2028

Section	Changes
Whole policy	Previous ICT Acceptable Use Policy rewritten and renamed Online Safety and Acceptable Use of Technology Policy. Policy updated to reflect current expectations around online safety, filtering and monitoring, mobile phones, smart devices, staff use of personal devices, pupil image capture, school-owned devices, data protection, artificial intelligence and acceptable use by pupils and staff.
Mobile phones, smart devices and personal devices	Previous wording allowing pupil smart watches and mobile phones replaced with wording aligned to the school's Mobile Phones, Smart Devices and Image Capture Policy.
Image capture and pupil photographs	New wording added to confirm that staff must not use personal devices to take, store or share pupil photographs, videos or audio recordings, except in exceptional emergency circumstances.
Filtering and monitoring	New section added to reflect safeguarding expectations around filtering, monitoring and online safety.
Artificial intelligence and emerging technology	New section added to support safe, responsible and supervised use of AI and emerging technology in school.

Contents

1. Introduction.....	4
2. Scope.....	4
3. Use of Email.....	5
4. Roles and Responsibilities	5
5. Acceptable use of school technology.....	6
6. Pupil acceptable use.....	7
7. Staff acceptable use	8
8. Mobile phones, smart devices and personal devices.....	8
9. School-owned image capture devices	9
10. Email, messaging and communication.....	9
11. Social media and online platforms	9
12. Filtering and monitoring	10
13. Artificial intelligence and emerging technology	11
14. Data protection, passwords and security.....	12
15. Remote learning and video calls	13
16. Reporting concerns and breaches	14
17. Monitoring and review	15
Appendix 1: Staff, Governor, Volunteer, Visitor and Contractor Acceptable Use Agreement.....	16
Appendix 2: Pupil Acceptable Use Agreement.....	18
Appendix 3: Parent/Carer Summary	19

St John's C of E Primary School

Online Safety and Acceptable Use of Technology Policy

Our Vision

Learn Together • Achieve Together • Celebrate Together
'and let your light shine' – Matthew 5:16

Our Mission Statement

To enable all children to achieve their true potential in a caring and inclusive community based on Christian values

Our Values

Respect • Responsibility • Kindness • Perseverance • Truthfulness

1. Introduction

Technology is an important part of learning, communication and school life. At St John's C of E Primary School, we want pupils and staff to use technology positively, safely and responsibly.

Online safety is a safeguarding matter. Pupils can be exposed to risks through websites, apps, search engines, social media, online games, messaging, image sharing, artificial intelligence, mobile phones and smart devices. Staff also have professional responsibilities when using school technology, personal devices, email, social media, online platforms and pupil images.

This policy sets out the school's expectations for the acceptable use of technology by pupils, staff, governors, volunteers, visitors and contractors. It should be read alongside the school's safeguarding and child protection, behaviour management, data protection and mobile phones, smart devices and image Capture policies.

The school's aim is to ensure that technology is used in a way that:

- keeps pupils safe;
- supports learning;
- protects personal data;
- prevents misuse of personal devices;
- supports a calm and focused school environment;
- protects the reputation of the school;
- ensures staff understand their professional responsibilities;
- helps pupils learn how to use technology respectfully, safely and responsibly.

Failure to follow this policy may result in the withdrawal of access to school technology, behaviour consequences, safeguarding action, parent/carers contact, disciplinary action or other appropriate action, depending on the circumstances.

2. Scope

This policy applies to:

- pupils;
- staff;
- governors;
- volunteers;
- visitors;
- contractors;
- supply staff;
- anyone using school technology, school systems or school networks.

This policy applies to the use of:

- school computers, laptops and tablets;
- school-owned mobile devices;
- school-owned image capture devices;
- school networks, Wi-Fi and internet access;
- school email and communication systems;
- school websites and social media accounts;
- school-approved apps and platforms;
- online learning platforms;
- artificial intelligence and emerging technologies;
- personal devices when used on the school site or in connection with school business;
- photographs, videos and audio recordings.

3. Links with other Policies

This policy should be read alongside:

- Safeguarding and Child Protection Policy including Filtering and Monitoring Arrangements;
- Behaviour Management Policy;
- Mobile Phones, Smart Devices and Image Capture Policy;
- Code of Conduct;
- Data Protection Policy;
- Data Breach procedures;
- Records Management and Retention Policy;
- Anti-Bullying Policy;
- Harmful Sexual Behaviour / Child-on-Child Abuse Policy;
- RSHE Policy;
- Educational Visits Policy;
- Remote Learning Policy, where applicable.

Where there is any uncertainty, safeguarding and data protection expectations take priority.

4. Roles and Responsibilities

Governing Body

The Governing Body is responsible for:

- ensuring that the school has appropriate policies and procedures for online safety and acceptable use of technology;
- ensuring that online safety is treated as part of the school's safeguarding responsibilities;
- ensuring appropriate filtering and monitoring arrangements are in place and reviewed;
- ensuring that staff receive appropriate information and training;
- monitoring the effectiveness of this policy through safeguarding and leadership reporting.

Headteacher

The Headteacher is responsible for:

- ensuring this policy is implemented consistently;
- ensuring staff, pupils, parents/carers and visitors understand expectations;
- ensuring appropriate systems are in place for reporting and responding to concerns;
- ensuring staff have access to school-owned or school-approved devices where needed;
- ensuring that breaches are managed appropriately.

Designated Safeguarding Lead

The DSL is responsible for:

- leading on online safety as part of the school's safeguarding arrangements;
- responding to safeguarding concerns linked to technology, online behaviour, messages, images, recordings, mobile phones, smart devices and harmful content;

- ensuring staff know how to report online safety concerns;
- ensuring concerns are recorded appropriately;
- seeking advice from external agencies where required.

Staff

Staff are responsible for:

- following this policy and associated acceptable use of technology agreements;
- modelling safe, respectful and professional use of technology;
- using school technology and systems responsibly;
- not using personal devices to take, store or share pupil images or recordings;
- reporting online safety, safeguarding, data protection or security concerns promptly;
- supporting pupils to use technology safely and responsibly.

Pupils

Pupils are responsible for:

- using school technology safely and respectfully;
- following staff instructions;
- not using personal phones or smart devices on the school site;
- reporting anything online that worries or upsets them;
- treating others kindly and respectfully online.

Parents and carers

Parents and carers are responsible for:

- supporting the school's online safety and mobile phone expectations;
- ensuring pupils do not bring prohibited smart devices to school;
- contacting the school office rather than contacting pupils directly during the school day;
- supporting pupils to use technology safely and responsibly outside school.

Visitors, volunteers and contractors

Visitors, volunteers and contractors are responsible for:

- following school expectations for technology use;
- not using phones or smart devices in pupil areas unless agreed by the school;
- not taking photographs, videos or recordings of pupils on personal devices;
- reporting any safeguarding or online safety concerns immediately.

5. Acceptable use of school technology

School technology is provided to support teaching, learning, administration, safeguarding, communication and the effective running of the school.

All users must use school technology responsibly, professionally and in line with school policies, safeguarding expectations and data protection requirements.

School technology includes, but is not limited to:

- computers, laptops and tablets;
- school-owned mobile devices;
- school-owned image capture devices;
- school networks and Wi-Fi;
- school email accounts;
- school telephones and communication systems;
- school-approved apps and platforms;
- school websites and social media accounts;
- online learning platforms;
- school data systems;

- filtering and monitoring systems;
- printers, scanners and other connected devices.

Users must not use school technology, networks or systems to access, download, upload, send, receive, store, create, copy or distribute any material that is illegal, harmful, offensive, discriminatory, defamatory, malicious, pornographic, violent, extremist, bullying-related or otherwise inappropriate.

Users must not attempt to bypass school filtering, monitoring, security settings, passwords or access controls.

Users must not install software, apps, browser extensions or other tools onto school equipment or systems unless this has been authorised by the Headteacher, Deputy Headteacher or IT provider.

Users must not use school equipment, systems or accounts for personal commercial activity, personal financial gain, private tutoring, political campaigning, unauthorised fundraising, or activity that is inconsistent with the school's values, policies or professional expectations.

Incidental personal use of school technology may be permitted where this has been agreed or is reasonable, provided that it:

- does not interfere with school business;
- does not interfere with the user's duties;
- is reasonable in duration and frequency;
- takes place during authorised breaks or outside directed/working time;
- does not create additional cost or risk to the school;
- does not involve inappropriate, confidential or sensitive material;
- does not bring the school into disrepute.

The school may withdraw access to school technology, networks or systems where this policy is not followed.

6. Pupil acceptable use

Pupils are taught to use technology safely, respectfully and responsibly. Technology use in school must support learning and must take place under the direction or supervision of staff.

Pupils must:

- use school technology only when allowed by a member of staff;
- follow staff instructions when using devices, websites, apps or online platforms;
- use school technology for learning and agreed school purposes;
- treat others kindly and respectfully when using technology;
- tell an adult immediately if they see or receive anything online that worries, upsets or confuses them;
- tell an adult if someone sends them an unkind, inappropriate or worrying message;
- tell an adult if they accidentally access unsuitable content;
- keep passwords private;
- respect other people's work, files and accounts;
- use school devices carefully and report any damage or fault.

Pupils must not:

- use another person's login or password;
- access another person's files, work or account without permission;
- search for, access or share inappropriate, harmful or unsuitable content;
- send unkind, bullying, threatening or inappropriate messages;

- take photographs, videos or audio recordings unless a member of staff has given permission for a clear school purpose;
- share images, videos or recordings without permission;
- try to bypass filtering, monitoring or security systems;
- use school technology to access games, apps, websites or platforms that have not been allowed by staff;
- share personal information online;
- deliberately damage school devices or systems;
- use artificial intelligence tools unless directed and supervised by staff.

Any misuse of school technology may be dealt with under the Behaviour Management Policy, Safeguarding and Child Protection Policy, and Mobile Phones, Smart Devices and Image Capture Policy.

Where misuse raises a safeguarding concern, this must be reported to the DSL or DDSL immediately.

7. Staff acceptable use

Staff are expected to model safe, professional and responsible use of technology at all times.

Staff must use school technology, systems and accounts in a way that:

- supports their professional role;
- keeps pupils safe;
- protects confidential information and personal data;
- upholds the reputation of the school;
- complies with safeguarding, data protection and online safety requirements;
- reflects the school's vision and values.

Staff must use approved school systems for school business. School business must not be conducted through personal email accounts, personal messaging apps, personal social media accounts or other personal platforms.

Staff must not use school technology, systems or accounts to access, create, download, upload, store, send, receive or share material that is inappropriate, offensive, illegal, discriminatory, defamatory, harmful, extremist, sexualised, violent or otherwise unsuitable.

Staff must not use school technology for personal commercial purposes, personal financial gain, or any activity that creates a conflict of interest with their role in school.

Staff must not share school passwords or allow pupils, family members or unauthorised individuals to access school accounts, systems or devices.

Staff must lock devices or log out when leaving them unattended.

Staff must report any loss, damage, unauthorised access, data breach, cyber security concern or online safety concern as soon as possible to the Headteacher, DSL, School Business Manager, IT provider or Data Protection Officer as appropriate.

8. Mobile phones, smart devices and personal devices

All staff, pupils, volunteers, visitors and contractors must follow the school's Mobile Phones, Smart Devices and Image Capture Policy.

9. School-owned image capture devices

The school will provide school-owned or school-approved devices for taking photographs, videos or audio recordings of pupils for agreed school purposes in accordance with the school's Mobile Phones, Smart Devices and Image Capture Policy.

10. Email, messaging and communication

School business must be conducted through approved school communication systems.

These may include:

- school email accounts;
- school telephones;
- the school office;
- approved school communication platforms;
- approved learning platforms;
- approved school social media accounts, where authorised.

Staff must not use personal email accounts, personal messaging apps, personal social media accounts or personal phone numbers to communicate with pupils or parents/carers about school matters.

Staff must not give pupils personal contact details, including personal phone numbers, personal email addresses, personal social media accounts, gaming usernames or messaging app details.

Emails and electronic messages must be professional, accurate, respectful and in line with the school's values. Staff should remember that emails and messages may be disclosed as part of complaints, safeguarding processes, subject access requests, legal processes or internal investigations.

Staff must take care when sending emails or messages containing personal data. Before sending, staff should check:

- the recipient;
- the attachment;
- whether the information is necessary;
- whether the information is being sent through an approved system;
- whether any sensitive information is appropriately protected.

Staff must not send, forward or respond to messages that are defamatory, offensive, discriminatory, bullying-related, sexualised, obscene, threatening or otherwise inappropriate. If such a message is received, staff must not forward it and must report it to the Headteacher, DSL, School Business Manager, IT provider or Data Protection Officer as appropriate.

Staff must take particular care with attachments, links and emails from unknown or unexpected senders, as these may contain viruses, malware, phishing attempts or other cyber security risks.

Pupils must only communicate online using school-approved systems and under the direction or supervision of staff. Pupils must not use school systems to send unkind, threatening, bullying, inappropriate or personal messages.

11. Social media and online platforms

Social media and online platforms include, but are not limited to:

- Facebook;
- Instagram;
- X;

- TikTok;
- YouTube;
- WhatsApp;
- Snapchat;
- LinkedIn;
- blogs;
- forums;
- gaming platforms;
- media sharing services;
- messaging apps;
- any other online platform where content can be created, shared, commented on or viewed by others.

Only SLT and teaching staff may post on or manage official school social media accounts or online platforms.

Official school accounts must:

- use approved school login details and school email addresses;
- be managed in line with safeguarding and data protection expectations;
- use appropriate privacy and security settings;
- reflect the school's vision and values;
- be professional in tone and content;
- avoid unnecessary personal data;
- follow the school's photo consent and opt-out arrangements, which are recorded on the school's MIS system;
- be monitored appropriately.

Before any image, video or recording of a pupil is used on the school website, social media, newsletters, printed publications or other external communication, staff must check the consent information recorded on the school's MIS system or confirm this with the school office/SLT.

Staff must not post, upload, comment on, discuss or share school-related information, pupil information, parent/carer information, staff information, confidential matters, complaints, safeguarding issues or internal school business on personal social media accounts or personal online platforms.

Staff must not use personal social media or messaging platforms to contact pupils.

Staff should avoid personal online contact with former pupils, particularly those under the age of 18. Any contact with former pupils must be appropriate, justifiable and, where necessary, agreed with school leaders and conducted through professional channels.

Staff must not access, follow, monitor or interact with pupils' personal social media accounts, unless there is a clear safeguarding reason and this has been agreed with the DSL or Headteacher.

Staff should be aware that personal social media use may affect the reputation of the school or call into question their suitability to work with children, even where privacy settings are used.

The school may require the removal of online content where it considers that the content is inappropriate, breaches school policy, compromises safeguarding or data protection, or brings the school into disrepute.

12. Filtering and monitoring

The school recognises that filtering and monitoring are part of its safeguarding responsibilities.

The school will maintain appropriate filtering and monitoring systems to help protect pupils from harmful or inappropriate online content when using school networks and devices.

Filtering and monitoring arrangements will be reviewed at least annually and whenever there is a significant change to technology, systems, safeguarding risks or school provision.

The review will consider:

- whether the filtering system is appropriate for the age and needs of pupils;
- whether monitoring arrangements are effective;
- whether staff understand how to report concerns;
- whether pupils are able to access appropriate learning resources;
- whether harmful content is being blocked appropriately;
- whether any groups of pupils may be at greater risk;
- whether emerging risks, including artificial intelligence, misinformation, disinformation and harmful online trends, have been considered.

Staff must report any concern that filtering or monitoring is not working effectively. This includes:

- pupils accessing inappropriate or harmful content;
- appropriate learning content being unnecessarily blocked;
- repeated attempts to access unsuitable content;
- concerns about searches, messages, images or online behaviour;
- concerns about online abuse, bullying, exploitation or harmful sexual behaviour;
- concerns about radicalisation, extremism or harmful misinformation.

Pupils are taught to report anything they see online that makes them feel worried, unsafe, uncomfortable or confused.

The DSL will be informed of filtering and monitoring concerns where there is a safeguarding implication.

The Headteacher, DSL, governing body, IT provider and relevant staff will work together to ensure filtering and monitoring remain effective and proportionate.

13. Artificial intelligence and emerging technology

The school recognises that artificial intelligence and emerging technologies can support learning, creativity and efficiency when used safely and responsibly. The school also recognises that these technologies may create risks linked to misinformation, bias, privacy, safeguarding, plagiarism, harmful content, image generation, impersonation and data protection.

Artificial intelligence tools must only be used in school where this has been approved or directed by staff. Pupils must not use artificial intelligence tools independently during the school day unless this is part of a planned and supervised learning activity.

Pupils must not use artificial intelligence or other technology to:

- create harmful, offensive, bullying-related, discriminatory or sexualised content;
- create or manipulate images of pupils, staff or other members of the school community;
- impersonate others;
- produce work dishonestly;
- bypass school expectations;
- access unsuitable or unsafe material;
- share personal or confidential information.

Staff must not enter personal, confidential or sensitive school information into artificial intelligence tools. This includes information about pupils, parents/carers, staff, governors, safeguarding, SEND, medical needs, behaviour, attendance, assessment, complaints, employment matters or any other identifiable or confidential school information.

This includes, but is not limited to:

- pupil names;
- staff names;
- safeguarding information;
- SEND information;
- medical information;
- behaviour records;
- assessment data;
- parent/carer information;
- confidential school documents;
- identifiable photographs, videos or recordings.

Staff may use artificial intelligence tools to support general drafting, planning, rewording, summarising, idea generation and administrative efficiency, provided that no personal, confidential, sensitive or identifiable school information is entered.

Any content produced using artificial intelligence must be checked carefully by staff before it is used or shared. AI-generated content may be inaccurate, biased, incomplete, inappropriate or out of date. Staff remain professionally responsible for any material they use or share.

Where the school wishes to use an AI tool for processing personal data or confidential school information, this must not happen unless it has been approved by the Headteacher and Data Protection Officer, a data protection assessment has been completed, and the use is reflected in the school's data protection documentation and privacy information.

14. Data protection, passwords and security

All users must follow the school's Data Protection Policy and data protection procedures.

Personal data must be handled lawfully, securely and only for legitimate school purposes. This includes information about pupils, parents/carers, staff, governors, volunteers and other members of the school community.

Personal data includes, but is not limited to:

- names and contact details;
- assessment information;
- attendance information;
- behaviour information;
- safeguarding information;
- SEND information;
- medical information;
- photographs, videos and audio recordings of identifiable individuals;
- staff employment information;
- parent/carer information.

Staff must take reasonable steps to keep school data secure. This includes:

- using strong passwords;
- keeping passwords confidential;

- locking screens or logging out when leaving devices unattended;
- storing devices securely;
- using approved school systems;
- avoiding unnecessary printing or downloading of personal data;
- not storing school data on personal devices;
- not uploading school data to personal cloud storage;
- not sending school data through personal email or personal messaging apps;
- checking recipients carefully before sending emails;
- reporting actual or suspected data breaches promptly.

Staff must not share passwords or allow pupils, family members or unauthorised individuals to use staff accounts, staff devices or unrestricted school systems.

Pupils must not share passwords or use another person's login details.

Any loss, theft, unauthorised access, accidental disclosure, misdirected email, missing device, inappropriate sharing of pupil information, or suspected data breach must be reported immediately in line with the school's Data Protection Policy and Data Breach procedures.

Photographs, videos and audio recordings of identifiable pupils are personal data. These must be taken, stored, shared and deleted in line with the school's Data Protection Policy, Mobile Phones, Smart Devices and Image Capture Policy, and parental consent arrangements.

15. Remote learning and video calls

Where remote learning, video calls or virtual meetings are used, the same standards of safeguarding, behaviour, data protection and professional conduct apply as they do in school.

Remote learning or virtual contact with pupils must only take place through school-approved platforms and systems.

Staff must not use personal accounts, personal email addresses, personal messaging apps or personal social media to communicate with pupils.

Virtual learning sessions or online meetings with pupils should:

- be agreed and approved by the school;
- use school-approved systems;
- be for a clear educational or school purpose;
- take place at appropriate times;
- be conducted professionally;
- use appropriate language and tone;
- maintain professional boundaries;
- take place from an appropriate location;
- avoid personal or private spaces where possible;
- ensure that background images, objects or other visible material are appropriate;
- follow school safeguarding expectations.

Where one-to-one virtual contact is necessary, this must be agreed in advance and managed in line with safeguarding procedures. Where appropriate, another adult should be present or aware of the arrangement.

Staff and pupils should dress appropriately for virtual learning or online meetings.

Staff must not record virtual sessions unless this has been agreed by the Headteacher or DSL and there is a clear school purpose. Where recording is agreed, participants must be informed, and the recording must be stored securely on approved school systems.

Any safeguarding, behaviour, online safety or data protection concern arising during remote learning or a video call must be reported immediately in line with school procedures.

16. Reporting concerns and breaches

All members of the school community have a responsibility to report concerns about online safety, technology use, data protection, mobile phones, smart devices, images, recordings, filtering, monitoring or cyber security.

Pupils should report concerns to a trusted adult.

Staff must report concerns promptly to the appropriate person. This may include the:

- Headteacher;
- Designated Safeguarding Lead;
- Deputy Designated Safeguarding Lead;
- School Business Manager;
- Data Protection Officer;
- IT provider;
- line manager.

Concerns may include, but are not limited to:

- pupils accessing harmful or inappropriate content;
- online bullying or harassment;
- inappropriate messages;
- sharing or requesting images;
- nude or semi-nude images;
- grooming or exploitation concerns;
- harmful sexual behaviour online;
- radicalisation or extremist content;
- misuse of mobile phones or smart devices;
- misuse of school technology;
- use of personal devices contrary to school policy;
- staff, visitor or volunteer misuse of technology;
- data breaches;
- loss or theft of devices;
- unauthorised access to accounts or systems;
- cyber security concerns;
- attempts to bypass filtering or monitoring;
- concerns linked to artificial intelligence or emerging technology.

Where a concern involves a child's safety or welfare, it must be reported to the DSL or DDSL immediately and recorded in line with safeguarding procedures.

Where a concern involves a member of staff, volunteer, visitor or contractor, it must be reported in line with the Code of Conduct, Low-Level Concerns procedures, Whistleblowing Policy and Safeguarding and Child Protection Policy.

Where a concern involves personal data, it must be reported in line with the Data Protection Policy and Data Breach procedures.

The school will respond to breaches in a proportionate way. Depending on the nature of the concern, this may include:

- education or reminder of expectations;
- removal of access to school technology;
- behaviour consequence;
- parent/carer contact;
- confiscation of a device;
- safeguarding action;
- data protection action;
- referral to external agencies;
- staff management action;
- disciplinary action;
- police involvement where necessary.

17. Monitoring and review

The Headteacher and DSL will monitor the implementation of this policy.

The policy will be reviewed at least every two years, or sooner if there are changes to statutory guidance, safeguarding expectations, data protection requirements, technology, school systems or local circumstances.

Filtering and monitoring arrangements will be reviewed at least annually.

The Governing Body will monitor the effectiveness of this policy through safeguarding, behaviour, data protection and leadership reporting.

The school will seek to ensure that this policy remains practical, proportionate and workable for staff, while keeping pupils safe and protecting school data.

Appendix 1: Acceptable Use of Technology Agreement for Staff, Governors, Volunteers, Visitors and Contractors

This agreement applies to all staff, governors, volunteers, visitors and contractors who use school technology, school systems, school networks or personal devices in connection with school business.

I understand my professional responsibility when using ICT, school systems, data, email, the internet, mobile devices, smart devices, school-owned devices and related technologies at St John's C of E Primary School.

I agree that:

1. I will use school technology, systems, networks and accounts responsibly, professionally and only for agreed school purposes or reasonable use permitted by the Headteacher or Governing Body.
2. I understand that school network, internet and system use may be logged and monitored, and that information may be made available to the Headteacher or appropriate senior leader where there is a safeguarding, conduct, data protection, legal or operational reason.
3. I will only use approved school systems, school email accounts and school communication platforms for school business.
4. I will not use personal email accounts, personal messaging apps, personal social media accounts or personal phone numbers to communicate with pupils or parents/carers about school matters.
5. I will not give pupils my personal contact details, including personal phone number, personal email address, social media details, gaming usernames or messaging app details.
6. I will not access, download, upload, create, store, send, receive or share material that is illegal, offensive, discriminatory, defamatory, harmful, extremist, sexualised, violent, bullying-related or otherwise inappropriate.
7. I will not attempt to bypass school filtering, monitoring, security settings, passwords or access controls.
8. I will not install software, apps, extensions or other tools onto school devices or systems unless this has been authorised.
9. I will keep passwords secure and will not share them with pupils, colleagues, family members or unauthorised individuals.
10. I will lock devices or log out when leaving them unattended.
11. I will ensure that personal data is kept secure and is only used for legitimate school purposes.
12. I will only access, store or share school data through agreed school or governance systems and will take appropriate steps to keep information secure.
13. I will not save school data to personal cloud storage, personal messaging apps, personal social media or other unauthorised locations. Where school information is accessed on a personal device for an agreed school or governance purpose, I will ensure the device is secure and that documents are deleted when no longer needed.
14. I will report any actual or suspected data breach, loss of device, unauthorised access, cyber security concern or online safety concern as soon as possible.
15. I will not use school technology, systems or accounts for personal commercial purposes, personal financial gain, unauthorised private tutoring, political campaigning or any activity that could create a conflict of interest or bring the school into disrepute.
16. I will not post, upload, comment on, discuss or share confidential school information, pupil information, parent/carer information, staff information, complaints, safeguarding matters or internal school business on personal social media or personal online platforms.
17. I will only post on official school social media accounts or platforms if I have been authorised to do so.
18. I will check and follow the school's photo consent and opt-out arrangements before using pupil images externally, including in newsletters, on the school website, on social media, in printed publications or in the media.

19. I will not use personal mobile phones, personal tablets, personal smart watches, personal cameras or any other personal device to take, store, upload, send or share photographs, videos or audio recordings of pupils.
20. I will only use school-owned or school-approved devices and systems to take photographs, videos or audio recordings of pupils, and only for agreed school purposes.
21. I will upload pupil images and recordings to the approved school system as soon as reasonably practicable and delete them from the school-owned device once they are no longer needed on the device.
22. I understand that personal devices may only be used to capture pupil images or recordings in exceptional emergency circumstances where no school-owned device is available and where the use is necessary and proportionate. If this happens, I will inform the Headteacher, DSL or senior leader as soon as possible, transfer the image or recording to the approved school system, and delete it from the personal device, including from any recently deleted folder.
23. I will not use artificial intelligence tools to process personal, confidential, safeguarding, SEND, medical, behaviour, assessment or identifiable pupil/staff information unless this has been approved by the school and data protection implications have been considered.
24. I will report any concern involving online safety, technology use, pupil images, mobile phones, smart devices, harmful content, artificial intelligence, filtering, monitoring or cyber security to the appropriate person.
25. I will support pupils to use technology safely, respectfully and responsibly.
26. I understand that failure to follow this agreement may result in withdrawal of access to school systems, safeguarding action, data protection action, management action, disciplinary action, referral to external agencies, or other appropriate action depending on the circumstances.

Name: _____

Role: _____

Signature: _____

Date: _____

School representative: _____

Date: _____

Appendix 2: Pupil Acceptable Use of Technology Agreement

At St John's, we use technology to help us learn, create, communicate and stay safe.

I agree that when I use school technology:

1. I will use school devices, websites, apps and online platforms only when an adult says I can.
2. I will follow adult instructions when using technology.
3. I will use school technology for learning and agreed school activities.
4. I will be kind and respectful when using technology.
5. I will not send unkind, rude, threatening or upsetting messages.
6. I will not search for, open or share anything inappropriate, harmful or upsetting.
7. I will tell an adult straight away if I see something online that worries, upsets or confuses me.
8. I will tell an adult if someone sends me an unkind, inappropriate or worrying message.
9. I will keep my password private.
10. I will not use someone else's login, password, work, files or account.
11. I will not take photographs, videos or recordings unless an adult has told me I can for a school activity.
12. I will not share photographs, videos or recordings without permission.
13. I will not share personal information online.
14. I will not try to get around school filtering, monitoring or security systems.
15. I will not use games, apps, websites or online tools unless an adult has said I can.
16. I will not use artificial intelligence tools unless an adult has told me I can and is supervising the activity.
17. I will look after school devices and tell an adult if something is broken or not working.
18. I understand that St John's is a phone-free school site for pupils.
19. I understand that I must not bring smartphones, smart watches, internet-enabled watches, tablets, gaming devices or other smart devices to school.
20. If I have permission to bring a basic call-and-text phone for travel or safety reasons, I will switch it off before entering the school site, hand it in straight away and collect it at the end of the day.
21. I understand that if I do not follow these rules, adults may need to speak to me, contact my parent/carer, remove my access to technology, confiscate a device, or use the school behaviour or safeguarding procedures.

Pupil name: _____

Class: _____

Pupil signature: _____

Date: _____

Appendix 3: Parent/Carer Summary

At St John's C of E Primary School, we want pupils to use technology safely, responsibly and respectfully.

Technology is an important part of learning, but it also brings risks linked to online safety, personal data, mobile phones, image sharing, messaging, social media, artificial intelligence and smart devices.

Pupil use of school technology

Pupils are taught to use school technology safely and responsibly. They are expected to:

- follow adult instructions;
- use school devices and platforms for learning;
- treat others kindly and respectfully online;
- report anything online that worries or upsets them;
- keep passwords private;
- avoid sharing personal information;
- not take or share photographs, videos or recordings without permission.

Any misuse of school technology may be managed through the school's Behaviour Management Policy, Safeguarding and Child Protection Policy, Online Safety and Acceptable Use of Technology Policy, and Mobile Phones, Smart Devices and Image Capture Policy.

Mobile phones and smart devices

St John's is a phone-free school site for pupils.

Pupils are not permitted to bring smartphones, smart watches, internet-enabled watches, tablets, gaming devices or other smart communication or recording devices onto the school site.

Where a pupil has an agreed travel or safety reason for bringing a phone, this must be a basic call-and-text phone only. It must be switched off before entering the school site, handed in on arrival and collected at the end of the school day.

Parents/carers should not contact pupils directly on personal devices during the school day. If you need to contact your child, please contact the school office. If your child needs to contact you, this will be arranged through the school office.

Photographs and videos

The school may take photographs and videos of pupils for agreed school purposes, such as learning evidence, displays, newsletters, the school website, approved school social media, educational visits and school events.

The school will check parental consent and opt-out information recorded on the school's MIS system before using images externally.

Staff must not use personal phones or personal devices to take, store or share photographs, videos or recordings of pupils, except in exceptional emergency circumstances. School-owned or school-approved devices and systems will be used for pupil images and recordings.

Online safety

Pupils are taught about online safety through the curriculum and wider school life. This includes learning about:

- safe and respectful communication;
- online bullying;
- privacy and consent;

- image sharing;
- harmful content;
- misinformation;
- artificial intelligence;
- reporting worries or concerns.

Parents/carers can support this by talking to children about safe technology use at home, monitoring age-appropriate use of devices and apps, and informing the school if they become aware of an online safety concern involving pupils from the school.

Reporting concerns

Please contact the school in line with the concerns guidance if you are concerned about:

- online bullying;
- inappropriate messages;
- image sharing;
- unsafe use of devices;
- harmful online content;
- misuse of phones or smart devices;
- contact between pupils online that is worrying or inappropriate;
- any safeguarding concern linked to technology.