ICT and internet acceptable use policy

Our Christian Vision

Believe **A**chieve **R**espect **T**ogether **S**ucceed

B – We **believe** we will flourish in God's family.
A – We know that everyone in St Bart's can **achieve.**
R – We **respect** everyone in our family.
T – Together we support and help each other.
S – As part of God's family we support everybody to **succeed.**

Safeguarding

St Bartholomew's C of E Primary School is committed to safeguarding and promoting the welfare of its pupils. We believe all staff and visitors have an important and unique role to play in the protection of children.

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors.
- Establish clear expectations for the way all members of the school community engage with each other online.
- Support the school's policy on data protection, online safety and safeguarding.
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems.
- Support the school in teaching pupils safe and effective internet and ICT use.

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under the school's policies on behaviour and codes of practice.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018.
- The General Data Protection Regulation.
- Computer Misuse Act 1990.

- Human Rights Act 1998.
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
- Education Act 2011.
- Freedom of Information Act 2000.
- The Education and Inspections Act 2006.
- Keeping Children Safe in Education 2022.
- Searching, screening and confiscation: advice for schools.
- National Cyber Security Centre (NCSC).
- Education and Training (Welfare of Children Act) 2021.

3. <u>Definitions</u>

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose.
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities.
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

See appendix 6 for a glossary of cyber security terminology.

4. <u>Unacceptable use</u>

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.1 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright.
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Online gambling, inappropriate advertising, phishing and/or financial scams.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful.

- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery).
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, its pupils, or other members of the school community.
- Connecting any device to the school's ICT network without approval from authorised personnel.
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities.
- Causing intentional damage to ICT facilities.
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour and codes of practice.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's ICT Technician manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices.
- Access permissions for certain programmes or files.

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT Technician.

5.1.1 Use of phones and email

- The school provides each member of staff with an email address.
- This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email accounts.
- All work-related business should be conducted using the email address the school has provided.
- Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- If staff send an email in error that contains the personal information of another person, they must inform the ICT Technician and Business Manager immediately and follow our data breach procedure.
- Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.
- School phones must not be used for personal matters.
- Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching hours.

- Does not constitute ‘unacceptable use’, as defined in section 4.
- Takes place when no pupils are present.
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes.
- Staff may not use the school’s ICT facilities to store personal non-work-related information or materials (such as music, videos or photos).
- Staff should be aware that use of the school’s ICT facilities for personal use may put personal communications within the scope of the school’s ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.
- Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.
- Staff should take care to follow the school’s guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Remote access

Remote access is available to the ICT technician and School Business Manager. This allows them to remotely login to their desktop computer at school.

The software used to allow this is Anydesk. Anydesk has two levels of security:

- Level One – Once installed on a machine in school, Anydesk assigns a randomly generated number to that machine. Access to the desktop is only allowed using the correct generated number.
- Level Two – Once the connection is established, the user has to input their correct school network username and password on the machine in order to login and use the school network.

Staff accessing the school’s ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be vigilant if they use the school’s ICT facilities outside the school and not share their Anydesk number or school network username and password.

Our ICT facilities contain information that is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

Requests for remote access will only be granted with approval of the ICT Technician, headteacher and deputy headteacher.

5.4 School social media accounts

- The school has an official Facebook and Twitter page, managed by the ICT Technician. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.
- The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited.
- Bandwidth usage.
- Email accounts.
- Telephone calls.
- User activity/access logs.
- Any other electronic communications.
- Only authorised staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business.
- Investigate compliance with school policies, procedures and standards.
- Ensure effective school and ICT operation.
- Conduct training or quality control exercises.
- Prevent or detect crime.
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

6. Pupils

6.1 Access to ICT facilities

- Laptops and I Pads are available to pupils only under the supervision of staff.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules. Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright.
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery).
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, other pupils, or other members of the school community.
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities.
- Causing intentional damage to ICT facilities or materials.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We encourage all parents to remain respectful towards the school and its staff at all times, including online.

8. Data Security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

- Staff users of the school's ICT facilities set their own password. They have to renew their password every 90 days.
- The password they set has to contain 3 of the following:
    - Capital Letter
    - Lowercase Letter
    - Number
    - Special Character
- Staff users are responsible for the security of their accounts and passwords.
- Members of staff who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access revoked.
- Pupils are allocated usernames and passwords at the beginning of each school year. Each child has their own unique username and password which matches their Times Table Rock Star account.

8.2 Software updates, firewalls and anti-virus software

- All of the school's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.
- Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.
- Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

- All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.
- The school's data protection policy can be found on the school website (School Info, Policies).

8.4 Access to facilities and materials

- All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.
- These access rights are managed by the ICT Technician.
- Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user

should not have access to is shared with them, they should alert the ICT Technician immediately.

- Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

- The school ensures that its devices and systems have an appropriate level of encryption.
- School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.
- Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT Technician.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.
The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure.
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
  - Check the sender address in an email.
  - Respond to a request for bank details, personal information or login details.
  - Verify requests for payments or changes to information.
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents.
- Investigate whether our IT software needs updating or replacing to be more secure.
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data.
- Put controls in place that are:
  - Multi-layered – Anti Virus Software / Firewall Filtering (Talk Straight Netsweeper Agent) / Staff Email Phishing Awareness.
  - Up to Date – Dedicated server (Microsoft WSUS and Apple MAC Mini) to deliver software updates to networked machines and iPads.
  - Regularly Reviewed and Tested – ICT Technician regularly checks pupil laptops / iPads to ensure specific websites and search terms are blocked by the firewall filtering.
- Backup Critical Data:
  - Daily (1 x onsite backup / 1 x cloud backup)
    - Two USB Drives used onsite (Rotated daily) kept in two separate secure locations within school.
- Delegate specific responsibility for maintaining the security of our management information system (SIMS) to School ICT Services and the onsite ICT Technician.

- Ensure the ICT Technician conducts regular access reviews to make sure each user in the school has the correct level of permissions and admin rights.
- Develop and review periodically a disaster recovery information and procedure with the ICT Technician on how the school will react to an emergency response situation should major systems / communications fail. See Disaster Recovery Information & Procedure document.

10. Internet access

- The school wireless internet connection is secured using a password.
- All devices connected to the schools network access the internet through the firewall filtering system (Talk Straight Netsweeper).

10.1 – Pupils

- Pupils only use laptops and iPads supplied by school to access the internet.
- A piece of software called 'Netsweeper' is installed on all school laptops. This checks the user logging on against the group they are in on the school's domain controller server. The correct filtering level is then assigned depending on the group that user is in on the server.
- All pupil iPads are assigned an IP address in a specific range. The default filter for these IP addresses is the pupil filter.
- Pupil filtering is the most restrictive and blocks access to sites such as Facebook, Twitter, YouTube, Instagram and many more.

10.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA).
- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan).
- Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The headteacher and ICT Technician monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed at the end of every academic year by the Headteacher and Deputy Headteacher. At every review, the policy will be shared with the governing board.

12. Related policies

This policy should be read alongside the school's policies on:

- Online safety

- Safeguarding and child protection
- Behaviour
- Staff discipline (Staff Handbook)
- Data protection
- Remote education

Appendix 1: Facebook cheat sheet for staff

Don’t accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don’t share anything publicly that you wouldn’t be just as happy showing your pupils
6. Don’t use social media sites during school hours
7. Don’t make comments about your job, your colleagues, our school or your pupils online – once it’s out there, it’s out there
8. Don’t associate yourself with the school on your profile (e.g. by setting it as your workplace, or by ‘checking in’ at a school event)
9. Don’t link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

Change the visibility of your posts and photos to **‘Friends only’**, rather than ‘Friends of friends’. Otherwise, pupils and their families may still be able to read your posts, see things you’ve shared and look at your pictures if they’re friends with anybody on your contacts list

Don’t forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

The public may still be able to see posts you’ve **‘liked’**, even if your profile settings are private, because this depends on the privacy settings of the original poster

Google your name to see what information about you is visible to the public

Prevent search engines from indexing your profile so that people can’t **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if…

A pupil adds you on social media

In the first instance, ignore and delete the request. Block the pupil from viewing your profile

Check your privacy settings again, and consider changing your display name or profile picture

If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages

Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

It is at your discretion whether to respond. Bear in mind that:

Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school

Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

Do not retaliate or respond in any way

Save evidence of any abuse by taking screenshots and recording the time and date it occurred

Report the material to Facebook or the relevant social network and ask them to remove it

If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material

If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: staff, governors, volunteers and visitors

St Bartholomew's C of E Primary School

Acceptable usage of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

ICT and related technologies, such as computers, interactive whiteboards, e-mail, the Internet and mobile devices, are an expected part of our daily working life in school.

This agreement is based on the main statements concerning members of staff which form part of the school's Online Safety Policy.

To ensure that members of staff are fully aware of their professional responsibilities when using any form of Information & Communication Technology all staff are expected to comply with and sign this agreement

Any concerns or clarification should be discussed with the Headteacher, or ICT Technician.

A company called 'Talk Straight' are responsible for our internet connection as well as our school filtering system. On all laptops there is a small piece of software that detects whether a user is a pupil or staff when they logon. Appropriate filtering is then applied that dictates what content a user is allowed to view when browsing the internet.

I understand that

- ICT includes a wide range of systems, including; computer networks, laptops, mobile phones, PDAs, digital cameras, e-mail, the Internet.
- It may be a criminal offence to use a school ICT system for purposes not permitted by its owner.
- Failure to comply with this policy may result in sanctions being imposed, formal disciplinary action being taken or illegal use being reported to the appropriate authorities.
- All my use of any school computer network and the Talk straight will be logged.
- The school may exercise its right to monitor my use of the school's ICT systems, including; hardware, software, Internet access and e-mail.
- The Headteacher may designate a member of staff to delete any of my files, including e-mail, where they believe that unauthorized use of the school's information system may be taking place, or it may be being used for illegal purposes.
- Digital copies of images of pupils and / or staff may only be taken, stored and used for professional purposes, in line with the school's policy on the taking and use of photographs. Digital copies of images of pupils and / or staff must not be e-mailed or distributed outside the school without the permission of the Head teacher.

I will

- Comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- Only use the school's ICT systems (including hardware, software, email, Internet, Intranet, Learning Platform) and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or the Governing Body.
- Ensure that all electronic communications with pupils, parents and staff are compatible with my professional role.
- Take all reasonable steps to ensure that school data is stored securely and used appropriately, whether in school, taken off school premises or accessed remotely.
- Respect copyright and intellectual property rights.
- Support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- Report any accidental misuse of school ICT, or accidental access to inappropriate material, to the headteacher, Designated Safeguarding Lead, or ICT Technician.
- Immediately inform the headteacher or ICT Technician if I receive any offensive e-mail.
- Report any incidents of concern regarding children's safe use of ICT to the headteacher, Designated Safeguarding Lead, or ICT Technician.

I will not

- Use any school ICT for any purpose that could be deemed illegal, inappropriate, unprofessional, racist, hateful, or harassment.
- Browse, download, upload or distribute any material that could be considered offensive, pornographic, obscene, illegal or discriminatory.
- Allow anyone else to use a computer when I have logged on using my own username.
- Allow anyone else to use my username and password.
- Deliberately circumvent the school or Talk straight security and filtering systems.
- E-mail pupils, or allow pupils to e-mail me, using my own personal email account.
- Use YouTube, or similar websites, live, without vetting the content when pupils are present.
- Use FaceBook or similar websites when pupils are present, or encourage pupils to use them at school or home.
- Access the internet other than through the Talk straight network whilst on school premises.
- Install any hardware or software - I will see the ICT technician.
- Connect any personal laptop to any school system unless it has up-to-date antivirus protection.
- Use External USB Hard Drives or memory sticks to store school data that if lost could breach GDPR legislation (Personal information etc).

I have read the above and agree to comply with this code of conduct

Signature ………………………………………………………….

Date ………………………………………………………….

Full Name ……………………………………......................... (printed)

Appendix 3: Code of conduct for the acceptable use of ICT: KS1 pupils

St Bartholomew's C of E
Primary School

Code of conduct for the acceptable use of ICT facilities and internet

Year 1 and Year 2 Pupils

The school uses ICT to help me with my learning.
The school does its best to keep me safe when I am using ICT.

This is part of my learning about E-Safety.

I understand that

- **The school makes these rules so as to be fair to everyone.**
- **The school will keep a record of everything I do on the school computers.**
- **If I deliberately break these rules I will get into trouble.**

I will

- **Always ask permission from a member of staff before I use any ICT equipment in school.**
- **Use school ICT in a sensible and responsible way.**
- **Only use my own username and password when I log on to a school computer.**
- **Tell a member of staff straight away if I accidentally do something that I know I am not supposed to do with school ICT equipment.**
- **Tell a member of staff if I see anything on a school computer that upsets me or I do not like.**

I will not

- **Use a mobile phone at school.**
- **Deliberately use ICT to cause harm or be nasty to another person.**

Full name ……………………………………………………………..…

Class ……………………………………………………………..…

Date ………………….……..

Appendix 4: Code of conduct for the acceptable use of ICT: KS2 pupils

St Bartholomew's C of E
Primary School

Code of conduct for the acceptable use of ICT
Year 3, Year 4, Year 5 and Year 6 Pupils

The school uses ICT to help me with my learning.
The school does its best to keep me safe when I am using ICT.

This is part of my learning about E-Safety.

I understand that

- **The school makes these rules to keep me, my family and my friends safe.**
- **The school makes these rules so as to be fair to everyone.**
- **The school will keep a record of everything I do on the school computers, the Internet sites I visit and all my e-mails.**
- **If I deliberately break these rules I will be sanctioned, my parents/carers may be told and I may not be allowed to use school ICT equipment.**

I will

- **Always ask permission from a member of staff before I use any ICT equipment in school.**
- **Always ask permission from a teacher before I use the Internet or use e-mail.**
- **Use school ICT in a sensible and responsible way.**
- **Do my best to look after school ICT equipment properly.**
- **Only use my own username and password when I log on to a school computer.**
- **Follow the school's "Rules for Responsible Internet Use" when I am using the Internet.**
- **Save my work in my own user area on the school network.**
- **Ask permission before I save any work.**
- **Tell a member of staff straight away if I accidentally do something that I know I am not supposed to do with school ICT equipment.**
- **Tell a member of staff if I see anything on a school computer that upsets me or I do not like.**

I will not

- Use school equipment without permission.
- Use a mobile phone on school premises.
- Take digital photographs, or use a webcam, on school premises without permission from the Headteacher.
- Use computer equipment from home whilst on school premises.
- Use any computer disk or memory stick from home on any school computer.
- Use any other ICT equipment from home, including any games machine or console that has a built in camera, webcam, internet access or wireless connection.
- Use another person’s username and password.
- Deliberately look at other people’s computer files without permission.
- Deliberately use ICT to cause harm or be nasty to another person.

I agree to obey this code of conduct

Signature ……………………………………………………………..…

Class ……………………………………………………………..…

Date ………………………………………………………………

Full Name (printed) ………………………………..

Appendix 6: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank

TERM	DEFINITION
	details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it’s from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim’s computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user’s identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.