St Bartholomew's Church of England Primary School

Acceptable Use Policy

Action	Date
Document reviewed	September 2023
Reviewed By	Sarah Irvine
Adopted by Governors	September 2023
Next Review Date	September 2024

St Bartholomew's C of E (VA) Primary School

Follow Jesus in all we do.

School Vision

We seek to ensure that by following Jesus, each individual is inspired to shine in all areas of their educational and spiritual development.

'For I know the plans I have for you," declares the LORD, "plans to prosper you and not to harm you, plans to give you hope and a future.' (Jeremiah 29:11)

Mission Statement

Follow Jesus in all we do.

'When Jesus spoke again to the people, he said, "I am the light of the world. Whoever follows me will never walk in darkness but will have the light of life."' (John 8:12)

Core Values

Our school is underpinned by 6 core values

Courage
'Be strong and courageous; do not be frightened or dismayed, for the Lord your God is with you wherever you go.' (Joshua 1.9)

Friendship
'Love each other as I have loved you.' (John 15:12)

Service
'Serve one another in love' (Galatians 5.13)

Forgiveness
'Do not judge, and you will not be judged. Do not condemn, and you will not be condemned. Forgive, and you will be forgiven' (Luke 6:37)

Justice
'And what does the LORD require of you? To act justly and to love mercy and to walk humbly with your God.' (Micah 6:9)

Love
'Give thanks to the Lord, for he is good; his love endures forever.' (Chronicles 16:34)

St Bartholomew's Church of England Primary School

Contents

1. Introduction and Vision

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users). Our policy is based on the Online Safety Guidance Document, provided by LGFL School E-Safety Policy Guidance 2014 and Lancashire Schools' ICT Centre (April 2013). Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings.

The Policy is organised in 5 main sections:

1. Policies and Practices
2. Infrastructure and Technology
3. Education and Training
4. Standards and Inspection
5. Appendices

Related School Documents

- Child Protection Policy
- Online Safety Policy
- Lancashire County Council ICT Security Framework for Schools

Vision

ICT (Information and Communication Technology) is an important resource to support learning and teaching, as well as playing a significant role in the everyday lives of children, young people and adults. Schools need to build in the use of these technologies in order to equip our young people with the skills to access life-long learning and employment. St Bartholomew's Church of England Primary School, aims to provide a diverse, balanced and relevant approach to the use of technology that gives our pupils both the skills and wisdom to use it to best effect.

We aim to:

- Through a variety of media, encourage the children to maximise the benefits and opportunities that technology has to offer.
- Ensure that children learn in an environment where security measures are balanced appropriately, with the need to learn effectively.
- Equip our pupils with the skills and knowledge to use technology appropriately and responsibly.
- Recognise the risks associated with technology and how to deal with them, both within and outside the school environment
- Ensure the users in the School Community understand why there is a need for an Online Safety Policy.

❖ The Role of the Online Safety Co-ordinator (Online Safety Champion)

The Role Includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's online safety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an online safety incident occur.
- Ensuring the online safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with online safety issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging online safety advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, SLT, staff, pupils and Governors are updated as necessary.
- Liaising closely with the school's Designated Senior Person / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

At St Bartholomew's Church of England Primary School, the Online Safety Co-ordinator is the, Headteacher.

❖ The School's Online Safety Webpage.

There is a comprehensive section on online safety on our School Website.

2. Policies and Practice

❖ Security and Data Management

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection
- All laptops and computers are password protected
- All children have their own password and are encouraged not to share it.

Data

All data in the school is kept secure and staff informed of what they can or can't do with data through the Online Safety Policy and statements in the Acceptable Use Policy (AUP).

- The Senior Leadership Team are responsible for managing information
- Staff are aware of where data is located
- All staff with access to personal data understand their responsibilities.
- The school ensures that data is appropriately managed both within and outside the school environment.
- The staff are aware that they should only use approved means to access, store and dispose of confidential data.
- Staff have access to school logins, to ensure their data remains secure.
- The school's policy on using mobile devices and removable media is that school information is not allowed to be carried on pen drives without password protection and no school data is allowed to be removed out of school on removable devices, for example pen drives that do not have password protection.
- The school aims to ensure that data loss is managed by the use of passwords for the required people.
- The school's procedure for backing up data is to use the internal server and LCC's remote back-up solution for office data.
- Children are not permitted to use staff laptops to ensure the confidentiality of data.

❖ Use of Mobile Devices

We strongly discourage children from bringing mobile phones into school. Should parents feel their child has a need to bring a phone into school it will be stored in the school office and collected at the end of the day. School cannot be responsible for any loss or damage caused to the mobile phone.

❖ Use of Digital Media

Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites.
To ensure all users are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media, any images taken at school will only be used for school purposes e.g. website, brochure or display.
In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below:

- At school photographs and video of pupils and staff are regarded as personal data in terms of The Data Protection Act (1998), and the school has written permission for their use from the individual and/or their parents or carers.
- the pupil, parent/carer or member of staff who appears in the media or whose name is used.

- The parental/carer permission is obtained on entry to school but parents have a right to change this if deemed necessary.
- The staff and pupils are aware that full names and personal details will not be used on any digital media, particularly in association with photographs.
- Parents/carers, who have been invited to attend school events are allowed to take videos and photographs if appropriate (videos are sometimes disallowed when the show is being recorded or when videoing by parents would cause inconvenience to others). Parents/carers should note that any videos or photographs taken are for personal use only and must not be placed on any social media site.
- All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites. See Social Media Policy
- The school ensures that photographs/videos are only taken using school equipment and only for school purposes.
- The school ensures that any photographs/videos are only accessible to the appropriate staff/pupils.
- Staff should not store digital content on personal equipment. Staff should not use their own cameras.
- When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
- Staff, parents/carers and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.

The guidelines for safe practice relating to the use of digital media, as outlined in the school's policy are monitored by the SLT and Governors on an annual basis.

❖ Communication Technologies

School uses a variety of communication technologies and is aware of the benefits and associated risks.

❖ Email

All users have access to the Lancashire Grid for Learning service as the preferred school e-mail system.

- Only official email addresses are used between staff and with pupils/parents when personal/sensitive data is involved.
- The Lancashire Grid for Learning Filtering Service, reduces the amount of spam (Junk Mail) received on school email accounts. Any significant incidents of spam should be reported to the ICT Helpdesk – BT Lancashire Service Education Team 0300 123 6797.
- All users are aware of the risks of accessing content including spam, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
- All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.

- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- Our school includes a standard disclaimer at the bottom of all outgoing emails (see next page).

St Bartholomew's Church of England Primary School email disclaimer:

All special in God's eyes

This e-mail and any files transmitted within it may be confidential and are intended for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent St. James' Lanehead C of E (VA) Primary School. If you are not the intended recipient, you must not use, disseminate, forward, print or copy this e-mail or its contents. If you have received this e-mail in error, please contact the sender. Please note that e-mail may be monitored in accordance with both school policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.

- **Social Networks**

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Twitter, Snapchat and Instagram. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users' content, send messages and leave comments.
All staff need to be aware of the following points:

- They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum.
- Pupils must never be added as 'friends' on any Social Network site.
- Children who are under 13 are not allowed to be members of Facebook under the Facebook recommendations.
- Staff are requested to change their profile picture to a 'generic' picture to avoid pupils contacting them through social networking sites such as Facebook.

Remember, whatever means of communication you use, you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Our school guidelines on using Facebook and other social media sites can be found in our Social Media Policy

These guidelines form part of this Acceptable Use Policy.

These guidelines will be circulated and discussed with staff at the start of every term. These are based on advice from Lancashire County Council Children and Young People's Directive.

❖ Mobile Telephone

- The school allows personal mobile phones on site but they must not be used at all during class time. Staff and visitors should ensure that mobile phones are switched off during curriculum time.
- If you are using your phone outside of curriculum time you should be in a place away from children, i.e. the staff room.
- Staff and visitors should not be on their own with a child and in possession of a mobile phone.
- Staff and visitors should not access our Wi-Fi system on their phone due to issues surrounding virus protection.
- It is acceptable to use personal mobile phones for school activities e.g. school trips. Do not take pictures of children on your personal mobile phone.
- Please refer to section mobile phones for guidance with children and mobile phones.

❖ Instant Messaging

Instant Messaging, e.g. MSN, Skype, Yahoo Messenger, WhatsApp and other similar services, is a popular communication tool with both adults and children. We do not currently use these communication tools at St Bartholomew's Church of England Primary School but will update this policy should we start to use them.

❖ Web Sites and other Online Publications

- The school website is effective in communicating online safety messages to parents/carers.
- Everybody in the school is made aware of the guidance for the use of digital media on the website page.
- Everybody in the school is aware of the guidance regarding personal information on the website.
- The school website is edited by all staff in School.
- The Head teacher has overall responsibility for what appears on the website.
- Parent/carer permission must be received before children's photos can appear on our website.
- User names and passwords must be kept private.

❖ Video Conferencing

Video conferencing is not currently used at St Bartholomew's Church of England Primary School.

- **Others**

The School will adapt/update the online safety policy in light of emerging new technologies and any issues or risks associated with these technologies e.g. Bluetooth and Infrared Communication.

- **Acceptable Use Policy (AUP)**

We have the following AUPs

- Staff and Governor Agreement
- Supply Teachers, Students and Visitors/Guests Agreement
- ICT School Acceptable Use Policy for Children (including parent/carer's agreement).

Our Acceptable Use Policies are intended to ensure that all users of technology within school will be responsible and stay safe. They ensure that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes. AUPs must be signed and adhered to by users before access to technology is allowed. The agreements are a partnership between parents/carers, pupils and the School to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology is kept in School and made available to all staff.

Our School AUP Aims to:

- Be understood by each individual user and relevant to their setting and purpose.
- Be regularly reviewed and updated annually.
- Be regularly communicated to all users, particularly when changes are made to the Online Safety Policy/AUP.
- Outline acceptable and unacceptable behaviour when using technologies, for example: Cyberbullying
- Inappropriate use of Email, Communication Technologies and Social Network sites and any Online content
- Acceptable behaviour when using school equipment /accessing the School Network.
- Outline the ways in which users are protected when using technologies e.g. passwords, virus protection and filtering.
- Provide advice for users on how to report any failings in technical safeguards.
- Clearly define how monitoring of network activity and online communications will take place and how this will be enforced.
- Outline sanctions for unacceptable use and make all users aware of the sanctions (linked to our Pastoral Policy).
- Stress the importance of online safety education and its practical implementation.
- Highlight the importance of parents/carers reading and discussing the content of the AUP with their child.

❖ Dealing with Incidents

The SLT is responsible for dealing with online safety incidents.

- Staff are aware of the different types of Online Safety incidents, (illegal and inappropriate) and how to respond appropriately.
- Children are informed of relevant procedures through discussions with members of staff.
- If a child reports an online safety incident to a teacher, the teacher should complete a blue online safety sheet and give it to the Online Safety Coordinator who will inform the Headteacher. If they are offsite, then the blue online safety should be given to the Headteacher or Deputy Headteacher.
- Incidents are logged in a log book kept in the Headteacher's Office.
- The above mentioned online safety Incident Log is monitored on a regular basis and reviewed by the Governing Body Health and Safety Committee.
- The SLT will decide at which point parents or external agencies are involved.
- The school uses the 'Online Safety Incident/ Escalation Procedures' document (See Appendix,) as a framework for responding to incidents.

❖ Illegal Offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher, who must refer this to external authorities, e.g. Police, CEOP, and Internet Watch
Foundation (IWF). Staff should never personally investigate, interfere with or share evidence as they may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Any potential illegal content would be reported to the Internet Watch Foundation. They are licensed to investigate – schools are not! (See Appendix 11).

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

More details regarding these categories can be found on the IWF website.

❖ Inappropriate Use

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and proportionate to the offence. The school will decide what constitutes inappropriate use and the sanctions to be applied. Some examples of inappropriate incidents are listed below with suggested sanctions.

❖ Accidental access to inappropriate materials:

- Minimise the webpage/ Turn the monitor off.
- Tell a trusted adult.
- Enter the details in the Incident Log and report to LGfL filtering services if necessary.
- Persistent 'accidental' offenders may need further disciplinary action.
- Using other people's logins and passwords maliciously / Deliberate searching for inappropriate materials / Bringing inappropriate electronic files from home / Using chats and forums in an inappropriate way.
- Inform SLT or designated online safety co-ordinator.
- Enter the details on a blue online safety sheet.
- Additional awareness raising of online safety issues and the AUP with individual child/class.
- More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy.
- Consider parent/carer involvement.

We will refer to the Lancashire School's ICT Centre advice on responding to an online safety incident.

3. Infrastructure and Technology

The school ensures that the infrastructure/network is as safe and secure as possible. Broadband connection, filtering and virus protection are provided (by default) by the Lancashire Grid for Learning.

❖ Pupil Access

The children are supervised by staff when accessing school equipment and online materials. Children are not allowed to use the computers and Internet unsupported at any time.

❖ Passwords

- All staff are aware of the guidelines in the Lancashire ICT Security Framework for Schools (see Appendix 12)
- All users of the school network have a secure username and password.
- The Administrator Password for the School Network is available to the Headteacher, School Business Manager and ICT Consultant and is kept in a secure place.
- Staff and pupils are reminded of the importance of keeping passwords secure.
- Passwords will only be changed if the need arises.

❖ Software/Hardware

- The school has legal ownership of all software.
- The school has an up to date record of appropriate licences for all software and the ICT consultant is responsible for maintaining this.

❖ Managing the network and technical support

- Servers, wireless systems and cabling are securely located and physical access restricted.
- The Headteacher is responsible for managing the security of the School Network.
- The safety and security of the School Network is monitored on a regular basis.
- The school systems are kept up to date in terms of security e.g. computers are regularly updated with critical software updates/patches.
- Users, (staff, pupils, guests), have clearly defined access rights to the school network e.g. they have a username and password.
- Staff and pupils are encouraged to lock, or log out, of a school system when a computer/digital device is left unattended.
- Only the administrator is allowed to download executable files and install software.
- Users report any suspicion or evidence of a breach of security to the SLT.
- The school does not permit staff/visitors to use removable storage devices on school equipment e.g. pen drives.
- The school encourages teachers to follow Online Safety Policy guidelines, when using laptop for personal/family use
- If network monitoring takes place, it is in accordance with the Data Protection Act (1998)
- All internal/external technical support providers are aware of your school's requirements /standards regarding online safety.
- The SLT and ICT Coordinator, are responsible for liaising with the ICT Consultant.

❖ Filtering and Virus Protection

St Bartholomew's Church of England Primary School, uses the LCC filtering system for school and regularly updates its virus software.

4. Education and Training

In 21st Century society, pupils need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.

The main areas of online safety risk that we need to consider:

Area of Risk.

Examples of Risk

Commerce

Pupils need to be taught to identify potential risks when using commercial sites. Advertising e.g. Spam. Privacy of Information (data protection, identity fraud, scams, phishing). Invasive software e.g. Virus', Trojans, Spyware Premium Rate services, Online gambling.

Content

Pupils need to be taught that not all content is appropriate or from a reliable source. Illegal materials, Inaccurate/bias materials, inappropriate materials, Copyright and plagiarism, User-generated content, e.g. YouTube, Flickr, Cyber-tattoo, Sexting.

Contact

Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.

Grooming. (including radicalisation)

Cyberbullying, Contact Inappropriate emails/instant messaging/blogging, encouraging inappropriate contact.

- **Online Safety Across the Curriculum**

It is vital that pupils are taught how to take a responsible approach to their own online safety.

St Bartholomew's Primary School, provides suitable online safety education to all pupils:

- Regular, planned online safety teaching within a range of curriculum areas (using the Lancashire ICT Progression framework).
- We will run discrete online safety days per year for children to focus on specific areas of online safety.
- Online safety education is differentiated for pupils with special educational needs.
- Pupils are made aware of the impact of Cyber-bullying and how to seek help if they are affected by these issues.
- Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- The school ensures that pupils develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of ICT both within and outside school.
- Pupils are reminded of safe Internet use e.g. classroom displays, online safety rules (See Appendices), acceptance of site policies when logging onto the school network / Moodle.

- **Online Safety - Raising Staff Awareness**

- All staff are regularly updated on their responsibilities as outlined in our school online safety policy.
- The online safety Co-ordinator provides advice/guidance or training to individuals as and when required.
- The online safety training ensures staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- All staff are expected to promote and model responsible use of ICT and digital resources.

- Online safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's Online Safety Policy and Acceptable Use Policy.
- Regular updates on Online Safety Policy, Acceptable Use Policy, curriculum resources and general online safety issues are discussed in staff/team meetings.

❖ Online Safety - Raising Parents/Carers Awareness

Parents often either underestimate, or do not realise how often children and young people come across potentially harmful and inappropriate material on the Internet and are often unsure about what they would do about it.
Byron Report, 2008.

The school offers opportunities for parents/carers and the wider community to be informed about online safety, including the benefits and risks of using various technologies. For example through:

- School Newsletters, Website and other publications.
- Promotion of external online safety resources/online materials.

❖ Online Safety - Raising Governors' Awareness

The school ensures that Governors, particularly those with specific responsibilities for online safety, ICT or child protection, are kept up to date on matters relating to online safety. This is through discussion at Governor Meetings, attendance at Local Authority Training, CEOP or internal staff/parent meetings.

The online safety Policy will be reviewed yearly (and/or if a serious breach occurs) by the online safety coordinator, approved by the governing body and made available on the school's website.

5. Standards and Inspection

Since September 2009 there has been greater emphasis on monitoring safeguarding procedures throughout schools.
At St Bartholomew's Church of England Primary School:

- Online safety incidents are monitored, recorded and reviewed.
- The SLT are responsible for monitoring, recording and reviewing incidents.
- The introduction of new technologies is risk assessed and these assessments are included in the online safety Policy as appropriate.
- Incidents are analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children.