St Bartholomew's Church of England Primary School

E Safety Policy

GDPR

Data will be processed to be in line with the requirements and protections set out in the UK General Data Protection Regulation.

Policy to be reviewed every 3 years
Reviewed by staff: M Applewhite 07/10/2025
Next review date: Autumn 2028

1. E Safety

Computing and Internet Safety in the 21st Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information. Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet – World Wide Web
- e-mail
- Instant messaging (often using simple web cams) e.g. Instant Messenger)
- Web based voice and video calling (e.g. Skype)
- Online chat rooms
- Online discussion forums
- Social networking sites (e.g. Facebook)
- Blogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (e.g. You Tube)
- Music and video downloading (e.g. iTunes)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access
- Online gaming

Our whole school approach to the safe use of Technology

Creating a safe Computing learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities
- E-Safety teaching is embedded into the school curriculum and schemes of work -- ***covering the 4 C's (content, contact, conduct and commerce)***

1.1 The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more so for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

1.2 As part of our commitment to learning and achievement we at St Bartholomew's CE Primary School want to ensure that the internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement and progress
- Uphold our Christian values *(X-Ref RE Policy)*
- Develop our creative curriculum and make learning exciting, fun and purposeful

- Enable pupils to gain access to a wide span of knowledge in a way that ensures and promotes their safety
- Enhance and enrich their lives
- Enable pupils to learn modern methods of communication to help them develop lifelong skills.

1.3 While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying *(X-Ref Anti Bullying Policy)*
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on social and emotional development and learning.
- Exposure to Artificial Intelligence and the dangers of false application of this technology can bring.

2. Introduction

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with and care for our children beyond the school environment (parents, carers, friends and the wider community) to be aware and to assist in this process.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school Computer systems, both in and out of school.

3. Acceptable Use Policies

All members of the school community are responsible for using the school computer systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

There are separate acceptable use policies for children and for all adults in school (teachers, governors and any adult volunteers). Acceptable use policies are revisited and resigned annually at the start of each school year and amended accordingly in light of new developments and discussions with the children which take place at the time. Copies are sent home for further discussion with parents and for children in EYFS and KS1 parents may sign on behalf of their children.

Staff and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy.

Parents sign once when their child enters the school, unless amendments have been made. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the school's computing resources (including the internet) and permission to publish their work. A copy of the pupil Acceptable Usage Policy is made available to parents at this stage and at the beginning of each year.

4. Cyber- bullying *(X-Ref Anti Bullying Policy)*

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

4.1 Child on child Abuse *(X-Ref Anti Bullying Policy and Safeguarding & Child Protection Policy)*

The school takes child on child abuse very seriously and considers that this is bullying- several times on purpose between fellow pupils. This would be dealt with in the same way as any serious bullying situation and would involve pupils and parents as necessary.

5. E-safety education

5.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of

pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

5.2 E-Safety education will be provided in the following ways:

- A planned e-safety programme has been put into place. Once these sessions have been delivered their impact on the children's e- safety awareness will be evaluated and the scheme revised and developed accordingly.
- We use the resources on Project Evolve website as a basis for our on-going e-safety education.
- Our key e-safety message of ZipIt! BlockIt! FlagIt! (created by the UK council for Child Internet Safety in 2009) is reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises throughout the curriculum and is displayed throughout the school, in classrooms and on device screens for regular reminders outside of the planned e-safety lessons
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of computing both within and outside school.
- In lessons where internet use is pre-planned, it is best and expected, practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit. No child should be left unsupervised when they are using the internet. Staff encourage the use of safe search engines to help filter the content and devices are set up to enable this to happen without the children requiring to go searching for these websites.
-

6. Plagiarism and Copywriting

Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:

- Checking the likely validity of the URL (web address)
- Cross checking references (can they find the same information on other sites?)
- Checking the 'pedigree' of the compilers/ owners of the website

Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Pupils are taught how to make best, and safe, use of internet search engines to arrive at the information they require

7. Staff Training

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required on an on-going basis
- It is expected that some staff will identify e-safety as a training need within the performance management process
- The E-Safety Coordinator will receive regular updates through attendance at local authority or other information / training sessions and by reviewing guidance documents released by the DfE, local authority and others
- Some reference will be made as part of the Child Protection /Safeguarding training

8. Governor Training

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee or group involved in computing, e-safety, health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, DLAT or Governor Development Services, National Governors Association or other bodies, in-house training delivered by staff
- Participation in school training / information sessions for staff or parents
- St Bartholomew's CE School have appointed an E-Safety Governor who will work closely with the E-Safety Coordinator completing an annual e- safety learning walk and providing updates and reports to the full governing body

9. Raising Parents and Carers Awareness

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. 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. "There is a generational digital divide". (Byron Report).

St Bartholomew's CE School will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters and our school website
- Parents evenings
- Reference to the parents materials on the Project Evolve website (www.thinkuknow.co.uk) or others
- Distribution of the recommended E- Safety publication 'Digital Parenting' from Vodafone
- Workshops or information evenings

10. Responsibilities:

E-Safety is recognised as an essential aspect of strategic leadership in this school and the SLT with the support of Governors, aims to embed safe practices into the culture of the school.

Leadership team

SLT ensures that the Policy is implemented across the school via the usual school monitoring procedures.

E-Safety Co-ordinator

Our school e-Safety Co-ordinator is Michael Applewhite.

He is responsible for keeping up to date on all e-Safety issues and ensuring that staff are updated as necessary.

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the e-Safety Policy.

School Staff

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. Staff should ensure they are familiar with the school e-Safety policy, and ask for clarification where needed. They should sign the Staff Acceptable Internet Use agreement annually. Class teachers should ensure that pupils are aware of the e-Safety rules, introducing them at the beginning of each new school year.

Pupils

Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with e-Safety issues, both at home and school. They are asked to agree to a set of guidelines and rules covering their responsibilities when using technology at school.

Parents

Parents are given information about the school's e-safety policy at the Admission interview. They are given copies of the pupil for information, and asked to support these rules with their children.

E-safety Coordinator

St Bartholomew's CE Primary School's E-Safety Coordinator is the person responsible to the SLT and governors for the day to day issues relating to e-safety. The E-Safety Coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school computing technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets with E-Safety Governor to discuss current issues, review incident logs and filtering change control logs
- attends relevant meetings and committees of Governing Body
- reports regularly to Senior Leadership Team
- receives appropriate training and support to fulfil their role effectively
- maintains logs of any occasions where the school has used its powers of search and deletion of electronic devices (eg. Looking at the 'history' on an iPad) alongside the computing technician

11. Responsibilities: Governors

Our governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors (or a governors' subcommittee) receiving regular information about e-safety incidents and monitoring reports. A member of the governing body has taken on the role of E-Safety Governor which involves:

- regular meetings with the E-Safety Co-ordinator with an agenda based on:
- monitoring of e-safety incident logs
- monitoring logs of any occasions where the school has used its powers of search and deletion of electronic devices (eg. Looking at the 'history' on an iPad)
- Carrying out an e-safety learning walk with the E-Safety Coordinator

- reporting to relevant Governors committee / meeting.

12. Responsibilities: Head teacher

The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Co-ordinator

The Head teacher and another member of the SLT should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff; see flow chart on dealing with e-safety incidents.

13. Responsibilities: Classroom Based Staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school's Acceptable Use Policy (AUP) for staff and are familiar with the children's AUP.
- they report any suspected misuse or problem to the E-Safety Co-ordinator
- digital communications with students (email / Remote learning) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in the curriculum and other school activities.
- St Bartholomew's School's Code of Conduct for the computers and the ZipIt! BlockIt! FlagIt! are prominently displayed and referred to in all classrooms

14. Responsibilities: Computing technician

The Computing Technician is responsible for ensuring that:

- the school's Computing infrastructure is secure and is not open to misuse or malicious attack
- users may only access the school's networks through a properly enforced password protection policy
- shortcomings in the infrastructure are reported to the Computing coordinator or SLT so that appropriate action may be taken.

15. Infrastructure

The filtering of internet content provides an important means of preventing our children and adults in school from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering

policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a school buying broadband services from Exa Networks we automatically receive the benefits of a managed filtering service via Surf Protect Filtering Services.

- **All users** have a responsibility to report immediately to class teachers / E-Safety Coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should be blocked.
- **Users** must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.
- **Pupils** are made aware of the importance of filtering systems through the school's e-safety education programme.
- **Staff** users will be made aware of the filtering systems through signing the AUP (a part of their induction process) and briefing in staff meetings, training days, memos etc. (from time to time and on-going).
- **Parents** will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions / newsletter etc.

16. Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images (illegal - The Protection of Children Act 1978)
- grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)
- possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)
- criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm

- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally the following activities are also considered unacceptable on computing equipment provided by the school:

- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Leicestershire County Council / or the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gambling and non-educational gaming
- Use of personal social networking sites / profiles for non-educational purposes

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

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 as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

17. Reporting of e-safety breaches

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

18. Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:

- Personal hand held devices will be used in lesson time **only** in an emergency or extreme circumstances
- **Staff should limit their use of personal mobile technologies to *necessary* communication only during specified breaks during the school day: at St Bartholomews CE Primary School this refers to the LUNCH BREAK only***
- *Exceptions to this are midday supervisors and staff on lunch duty who **SHOULD NOT** use personal mobile technologies during the lunch break at all
- Understand that personal mobile technologies **MUST BE SET TO SILENT** during the working day and should not be heard making any noise at all in any area of the school premises; this includes in classrooms, corridors, playgrounds, kitchen and offices
- Members of staff are free to use these devices in school, outside teaching time in accordance with the e-safety policy and the mobile digital equipment policy
- Pupils are not currently permitted to bring their personal hand held devices into school unless they have permission signed by a parent. These forms are held in the school office.

A number of such devices are available in school (e.g. iPads) and are used by children as considered appropriate by members of staff.

19. Email

Access to email is provided for all staff in school via the MS Outlook web page accessible via a web browser (internet Explorer) from their desktop.

These official school email services may be regarded as safe and secure and are monitored.

- Staff should use only the school email services to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email (see education section above)

- Staff may only access personal email accounts on school systems for emergency or extraordinary purposes (these may be blocked by filtering).
- Users must immediately report, to their class teacher / E-Safety Coordinator – in accordance with the school policy the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

20. Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission

See also the following section for guidance on publication of photographs

21. Use of web based publication tools

Our school uses the public facing website, St.Bartholomew's Church of England Primary School - Home (st-bartholomews.leics.sch.uk)sharing information with the community beyond our school. This includes celebrating work and achievements of children.

- Personal information should not be posted on the school website and only the official email address office@st-bartholomews.leics.sch.uk should be used to contact or identify members of staff (never pupils).
- Only pupil's first names are used on the website, and only then when necessary.
- Detailed personal calendars are not published on the school website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
- pupils' full names will not be used anywhere on a website or blog, and never in association with photographs

- Written permission from parents or carers will be obtained on admission into school before photographs of pupils are published on the school website.

22. **Professional standards for staff communication** *(cross reference Code of Conduct Policy)*

A teacher is expected to demonstrate consistently high standards of personal and professional conduct. The following statements from the Teaching Standards define the behaviour and attitudes which set the required standard for conduct throughout a teacher's career. Teachers uphold public trust in the profession and maintain high standards of ethics and behaviour, within and outside school, by:

- treating pupils with dignity, building relationships rooted in mutual respect, and at all times observing proper boundaries appropriate to a teacher's professional position

- having regard for the need to safeguard pupils' well-being, in accordance with statutory provisions

Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of pupils are used to inform this process also.

23. Areas for development

- Scheme of work to be analysed to work out how effectively it is being applied.
- Analysis of Yr 6 survey (over the last few years) to identify trends and school specific areas for development. Once identified, additional activities to be implemented to address these areas.