Fioretti Trust

ST BARNABAS C OF E PRIMARY SCHOOL

E- Safety and Acceptable Use Policy

"We encourage one another and build each other up, to be our best selves."

Proposed by: Melanie Bourne

Committee Responsible: Full Governing Board

Date Proposed: Spring Term 2024

Review Date: Spring Term 2027

Signed by Chair of Governors :

This policy supersedes all previous 'e-safety and acceptable use' policies.

1. Introduction

1.1 The Governing Body of St Barnabas Church of England School has adopted this policy to help the school meet its responsibilities for safeguarding and educating children, for regulating the conduct of employees and for complying with legislation covering the use of information and communication technologies and digital and mobile devices.

1.2 This policy was adopted by the Governing Body and will be reviewed bi -annually in the light of guidance from the local authority or earlier if the local authority issues further guidance in the light of particular circumstances or developments in information and communication technology.

The school will monitor and enforce the policy through:

- Teacher planning
- Securus XT – monitoring of network activity for laptops and desktops (mobile technology websites only covered)
- Log of any incidents (monitored by the DSL)
- Technical Staff to ensure all security software, including virus software and settings are kept up to date.

2. Basic principles

2.1 In adopting this policy the Governing Body has taken into account the expectation by Ofsted that rigorous e-safety policies and procedures are in place in the school, written in plain English, with contributions from the whole school, updated regularly and ratified by Governors.

2.2 The policy applies to all members of the school community, including staff, pupils, volunteers, parents and carers, Governors, visitors and community users who have access to, and are users of, the school's information and communication technology systems or who use their personal devices in relation to their work at the school.

2.3 The Governing Body expects the Head Teacher to ensure that this policy is implemented, that training in e-safety is given high priority across the school, that consultations on the details of the arrangements for e-safety continue with all employees on a regular basis, and that any necessary amendments to this policy are submitted to this Governing Body for approval.

2.4 The principal context for this policy is the need to safeguard children. It will be applied in conjunction with the procedure for safeguarding children approved by the Birmingham Safeguarding Children Board. It will also be applied in conjunction with the school's behaviour and anti-bullying policies for pupils and with the rules and procedures governing the conduct of employees.

2.5 The Governing Body expects the Head Teacher to arrange for this policy to be published to all employees and volunteers in the school and for necessary instructions and guidance, particularly on acceptable use, to be given to pupils in a manner suited to their ages and abilities.

3. Roles and responsibilities

Governing Body

3.1 The Governing Body will consider and ratify this e-safety policy, and review it annually in the light of guidance from the local authority, or sooner if the local authority issues new guidance in the light of particular circumstances or developments in information and communication technology. Governors are expected to follow the policy in the same way as volunteers are expected to follow it, including

participating in e-safety training if they use information and communication technology in their capacity as school Governors.

3.2 Governors are responsible for ensuring that proper procurement procedures are used if they decide to purchase information technology services from an external contractor and that City Council or other reputable specialist advice is taken on the specification for those services to ensure proper security and safeguarding of children.

Head Teacher

3.3 The Head Teacher is responsible for ensuring that

- the Governing Body is offered appropriate support to enable this policy and its application to be reviewed regularly, and to ensure that other school policies, including that on pupils' behaviour, take account of this e-safety policy;
- the Governing Body is given necessary advice on securing appropriate information and communication technology systems;
- the school obtains and follows City Council or other reputable guidance on information and communication technology to support this policy;
- the school has a designated senior person to co-ordinate e-safety and that this person has adequate support from, and provides support to, other employees, particularly the designated senior person for safeguarding;
- there is effective consultation with all employees, and other users of the school's information and communication technology systems, to take account of the particular features of those systems and educational, technical and administrative needs;
- the school provides all employees with training in e-safety relevant to their roles and responsibilities and that training is also provided to volunteers and school Governors who use information and communication technology in their capacity as volunteers or Governors, as the case may be;
- pupils are taught e-safety as an essential part of the curriculum;
- the senior leadership team is aware of the procedures to be followed in the event of a serious e-safety incident, including an allegation made against an employee, and that all employees know to whom they should report suspected misuse or a problem ;
- records are kept of all e-safety incidents and that these are reported to the senior leadership team;
- necessary steps have been taken to protect the technical infrastructure and meet technical requirements of the school's information and communication technology systems;
- there is appropriate supervision of, and support for, technical staff;
- any outside contractor which manages information technology for the school undertakes all the safety measures which would otherwise be the responsibility of the school to the standard required by the school and is fully aware of this policy and that any deficiencies are reported to the body which commissioned the contract.

Other employees

3.4 Other employees are responsible for

- undertaking such responsibilities as have been delegated by the Head Teacher commensurate with their salary grade and job descriptions;
- participating in training in e-safety provided by the school and in consultations about this policy and about its application, including e-safety within the curriculum;
- using information and communication technology in accordance with this policy and the training provided;
- reporting any suspected misuse or problem to the person designated by the school for this purpose.

Pupils

3.5 Pupils are expected to use information and communication technology systems and devices as they have been taught and in accordance with the school's behaviour policy and the instructions given to them by staff.

Other users

3.6 Volunteers, including Governors, who help in the school and who use information and communication technology systems and devices in helping the school are expected to

- participate in training in e-safety provided by the school and in consultations about this policy and about its application, including e-safety within the curriculum;
- use information and communication technology in accordance with this policy and the training provided;
- report any suspected misuse or problem to the person designated by the school for this purpose.

3.7 **Visitors to school**

Whilst the nature of a visitor's Internet use will clearly vary depending upon the purpose of their visit, it is still important to explain the school's expectations and rules regarding safe and appropriate Internet use to them. These differ slightly to those given to pupils to acknowledge the different situations in which visitors will likely be using the Internet:

- I will respect the facilities on offer by using them safely and appropriately.
- I will not use the Internet for: personal financial gain, political purposes, advertising, personal or private business.
- I will not deliberately seek out inappropriate websites.
- I will report any unpleasant material to a member of staff immediately because this will help protect myself and others.
- I will not download/install program files to prevent data from being corrupted and to minimise the risk of viruses.
- I will be polite and respect others when communicating over the Internet.
- I will not share my login details for websites with others.
- I will not carry out personal or unnecessary printing when using the Internet due to the high cost of ink.
- I understand that the school may check my computer files and monitor the Internet sites I visit.

These will be on a paper copy and signed by the visitor.

3.7 **Parents**

Parents who help in the school as volunteers are covered by 3.6 above. Parents who are not voluntary helpers in the school are nonetheless subject to the law in the event of misuse of information and communication technology.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities. Incidents that occur outside of school are covered by parent's duty of care.

3.8 **Curriculum**

Online Safety in the curriculum

A programme of training in online safety will be taught to children across the school from Nursery to Year 6. Online safety training will be included within the Personal Social and Health Education (PSHE) curriculum and children will be reminded at the beginning of any session using ICT.

Early Years Foundation Stage and Key Stage 1
At this level, use of the Internet will either be quite heavily supervised or based around pre-selected, safe websites. Children will be regularly reminded about how to always take care when clicking and to seek help/advice from an adult if they see anything that makes them unhappy or that they are unsure about. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult.

Lower Key Stage 2
Children will now be given more opportunities to develop their digital literacy skills (e.g. sending polite and friendly messages online to other children, the need to create strong passwords etc). They will be shown how to develop a responsible attitude towards searching the World Wide Web and will be reminded of the need to report any concerns they have. The importance of creating strong passwords and the benefits of only joining child-friendly websites will also be taught. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult.

Upper Key Stage 2
Children will now be encouraged to become more independent, agreeing to the acceptable use policy first, before searching for information on the World Wide Web using a child friendly search engine, being taught the necessary skills to critically evaluate sites for accuracy and suitability. They will be supported in using online collaboration tools more for communicating and sharing ideas with others, including being taught the need for not revealing personal information to strangers. The aim is to teach them how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult.

Monitoring Software
Securus XT is used across the network in order to:

- Monitor inappropriate use of language
- Monitor internet usage Inc. words associated with the prevent agenda
- Enforce the agreement of the Acceptable Use Policy

Managing filtering
Our ISP(EXA Networks) and Securus XT will work with us to ensure systems to protect pupils are reviewed. If staff come across unsuitable on-line materials, the site must be reported to the online safety Coordinator. If pupils come across unsuitable on-line materials, the site must be reported to their teacher who will inform the online safety Coordinator. Staff are able to access sites such as 'You Tube' and others on request but staff need to be aware that these sites do contain inappropriate materials and therefore children are not allowed to use these sites. Links and content should be checked in school just prior to use in the classroom due to daily rotation of advertising content.

Acceptable use

4.1 The use of information and communication technology should follow the following general principles:

- This policy should apply whether systems are being used on or off the school premises.
- The school's information and communication technology systems are intended primarily for educational use and the management and administration of the school. During work breaks appropriate, reasonable personal use is permitted.
- Data Protection legislation must be followed.
- Users must not try to use systems for any illegal purposes or materials.
- Users should communicate with others in a professional manner.

- Users must not disclose their password and they should not write it down or store it where it is possible that another person might steal it. Users must not attempt to use another person's user-name or password.
- Users must report as soon as possible any apparently illegal, inappropriate or harmful material or event to the person designated by the school.

4.2 Employees, volunteers and Governors should:

- not open, copy, remove or alter any other user's files without that person's express permission;
- only take and/or publish images of other people with their permission, or, in the case of pupils, the permission of their parents or guardians;
- when recording or publishing such images for educational purposes should not attach to those images any names or other personal information enabling identification;
- as far as possible communicate with pupils and parents only through the school's official communication systems and not publish personal contact details through those systems;
- if they occupy a senior post in which they need to keep e-mail and other messages confidential, ask the school for a separate e-mail address for this purpose;
- if they use personal devices during their work (subject to the agreement of the school in the case of employees), ensure that the systems which they use are secure, protected with passwords and encrypted;
- not use personal social networking sites through the school's information and communication technology systems;
- not open any hyperlinks in, or attachments to, e-mails, unless the source is known and trusted;
- ensure that their data is backed-up regularly in accordance with the rules of the school's systems;
- only download or upload large quantities of information if they have permission to do so, in order to avoid overloading the school's systems;
- not try to install any programmes or alter any computer settings unless this is allowed under the rules for the school's information and communication technology systems;
- not deliberately disable or damage any information and communication technology equipment;
- report any damage or faults to the appropriate member of staff.

4.3 **Social networking and personal publishing**

Use of social media networks or sites, whether by pupils or employees, should be subject to the same standards as the school would expect for behaviour and conduct generally (as set out in the school's code of conduct for support staff and the Teachers' Standards for teachers). The school accepts the separation of private life and work and will not concern itself with people's private lives unless it appears that the law has been broken, or that an employee is in breach of contract, or that the school is, or will be, brought into disrepute.

The school will control access to social networking sites, they will be restricted as appropriate. Pupils will be educated in the safe use of such sites alongside the use of relevant child friendly websites. Pupils, staff and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils. Pupils will be advised to use nicknames and avatars when using social networking sites. Staff must not make 'friends' or communicate with current pupils or pupils that have left on any social network site, i.e. Facebook. Staff should check that their privacy setting is set to 'Friends only' and consider changing their profile name. Staff who choose to use 'Facebook' and other network sites do so at their own risk and should be aware of the School's Code of Conduct. Pupils will be taught when 'gaming' i.e. on Nintendo Wii, Playstation, Xbox - they should only communicate with people they know rather than unknown gamers.

4.4 **Parents and Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. We will take every opportunity to help parents understand these

issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website / pupil records
- Their children's personal devices in the school (where this is allowed)

Where an incident occurs within school the child's parents will be given appropriate advice for the use of technology at home.

4.5 **E-communication within school**

Staff should use a school email communication for anything work related and no other email address. The forwarding of chain communications is not permitted.

4.4 **Mobile phones**

The use of mobile phones should not be in the classrooms especially during the school day (8.50 - 3.15) excluding lunchtimes in the staff room or office, and only used on school trips away from children, in an emergency.

4.5 **Digital images in the school community**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupil's instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images. Parents will be reminded of this at the beginning of any events where they are able to take images/videos.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow the school policy concerning the sharing, distribution and publication of those images which prohibits such activity. Those images should only be taken on 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 (e.g. school uniform or PE kit) 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. For example, a child must ask another before taking their photo.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names (First names and last initial only) will not be used anywhere on a website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

4.6 **Managing 21st century technologies**

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. School staff should be aware that mobile technologies with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Personal devices, including mobile phones, will not be used during lessons or formal school time unless express permission is given by the head or SLT. Personal devices must not be accessed (e.g. in another room or locked away) when children are present. The sending of abusive or inappropriate messages or files by Bluetooth or any other means is forbidden. Staff will be issued with a school phone where contact with pupils is required. Staff will not use personal devices to capture images/videos of pupils.

4.7 **Protecting personal data**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Refer to the School's data protection policy. Staff will be given access to a remote system to access data. This should be the only form of data storage that staff use. Staff should ensure that the device is not left unattended whilst logged in. Staff should not walk away from any device without first locking it.

5. Device loan for Remote Learning.

Technology plays a key role in maximising pupils' access to learning, as well as making lessons more exciting and interesting. We are committed to ensuring pupils have access to the necessary facilities to carry out their work at home if necessary. We believe it is important for pupils to be confident and competent users of equipment and the resources they allow access to. Staff, pupils and parents are expected to familiarise themselves with the school's online and acceptable use policy and to sign a device loan agreement before loaning any equipment. Copies of these will be made available on request.

5.1 **Device loan agreement – parents.**

This agreement will be between the school and the parent of the pupil who is loaned a school device or computing equipment. It is valid from the date that the device is issued until the date that the device is returned. The device remains the property of the school and is subject to the relevant school policies. This agreement has been created to establish the conditions by which the child may be loaned a device for the purposes of remote learning. It explains the expectation of acceptable use of the device to be adhered to by the child at all times. It should read and the agreement's conditions understood before consenting to the loan. If the conditions of this agreement are breached, the school may request that the device be returned immediately and parents may be liable for any damages or loss of property incurred. For the purpose of effectively administering its ICT systems against attack by viruses, spyware and hackers, the school reserves the right to scan, review and delete any files that may be held on its devices. This may, at times, necessitate the monitoring of the device and its internet activity; personal privacy and confidentiality will be strictly observed at all times.

5.2 **Acceptable use.**

The device or computing equipment belongs to the school and is provided on loan for your child's use; it should not be loaned out to anyone else or used by anyone else. The device is to be used for the purpose of remote learning only and not for personal use. The school may monitor a child's activity on the device.
The parents/ carers responsibilities include the following:

- Ensuring childrens activity on the device is overseen by an adult at all times.
- Preventing children from carrying out activity that is inappropriate and contrary to the device's intended purpose.
- Recognising that the school will manage a child's activity in line with the Behavioural Policy if they engage in unacceptable use, such as using offensive language, using the internet to bully someone and breaches in safeguarding.

● Ensuring the online safety of children on the device, e.g. setting parental controls on home broadband where necessary.
● Ensuring that children's activity on the device does not bring the school into disrepute, this includes the use of social media.
● Installing software on the device only with the prior agreement of the school.
● Ensuring that the device is not modified in any way, e.g. removing covers or disabling applications.
● Reporting any issues with the device to the school as soon as possible by phoning the office on 0121 464 5813

5.3 Loss or damage
By signing this agreement, parents and carers are accepting full responsibility for the device loaned to their child and acknowledging they understand the conditions of its use. The device will remain their responsibility until it has been returned to the school in the same condition that it was received. If the device suffers damage they should immediately contact the school. The school should be contacted along with the police where it is suspected stolen. Also taking responsibility for reasonable costs requested by the school to repair or replace the device where necessary. If difficulty is faced in reimbursing the costs of repair or replacement of the device, then the Head Teacher should be contacted on 0121 464 5813 to discuss the matter. In order to protect the device, following measures are observed:
● The device is not left unsupervised when in use
● The device is kept in a secure place when not in use
● The device is not left visibly on display in a car or at home
● The device is used appropriately, e.g. on a table
● No marks or decorations, e.g. stickers, are placed on the device
● No food or drink is consumed near the device

6. Handling Online safety complaints

Complaints of internet misuse will be dealt with by an e-safety coordinator or a senior member of staff. Any complaint about staff misuse must be referred to the LADO.

Complaints of a safeguarding nature must be dealt with in accordance with school's safeguarding procedures. Pupils and parents will be informed of consequences for pupils misusing the Internet.