

**BISHOP JOHN ROBINSON CHURCH OF ENGLAND PRIMARY  
SCHOOL**



## Online Safety Policy

**Be the best we can;**

**Join in learning, play and prayer,**

**Remember God's Word.**

Date of last review	September 2017
Ratified by Governors	September 2017
Next Review Date	September 2018
Designated Safeguarding Lead for Child Protection:	Ken Maslin - Head Teacher
Deputy Designated Safeguarding Lead for Child Protection:	Jo Richardson - Deputy Head Teacher
Named Governor for Safeguarding/Child Protection:	Susan Robinson

A handwritten signature in black ink, appearing to be 'KM' or 'Ken Maslin'.

A handwritten signature in black ink, appearing to be 'Jo Richardson'.

### Mission Statement

We want all adults and children to: **Be the best they can** in order to have best possible start in life and to make the most of the gifts God has given. To achieve this we;

- Set ambitious targets for all pupils and staff
- Continually look for ways to improve
- Have high expectations of behaviour for all

We encourage children to: **Join in Learning**, to promote academic excellence and to inspire everyone to value the importance of education in wider society. To achieve this we;

- Provide an engaging curriculum with opportunities for learning in a variety of contexts
- Strive for all lessons to be focussed and engaging to allow all children to achieve
- Support deeper levels of understanding so that children can apply learning to different settings

For children to: **Join in Play** is important at BJR because Play is essential for everyone's social and emotional development. It is a vital life skill which helps children to form the adult they will become building trust, forgiveness and resilience. To promote positive play we;

- Have dedicated staff who promote play EVERY PLAYTIME
- Promote the importance of play through PLAY DAYS
- Invest in the playground as a learning resource

We want the school community to: **Join in Prayer** as Christians believe that this is fundamental to developing a relationship with God as well as giving thanks and praise. We encourage this though;

- High quality collective worship for all children
- Daily acts of prayer
- Valuing the essential role of our School Chaplain

We believe that we should: **Remember God's Word**, as this is at the very Foundation of being a Christian school. In promoting a practical understanding and application of Christian Values we strive to; *"Train up a child in the way he should go, And when he is old he will not depart from it"* Proverbs 22:6 (NKJV) through;

- Providing High quality RE teaching and daily collective worship for all children
- Regular visits to church and other places of worship

## Contents

### 1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy is communicated to staff/pupils/community
- Handling complaints
- Reviewing and Monitoring

### 2. Education and Curriculum

- Pupil online safety curriculum
- Staff and governor training
- Parent awareness and training

### 3. Expected Conduct and Incident Management

### 4. Managing the IT Infrastructure

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking
- Video Conferencing

### 5. Data Security

- Management Information System access
- Data transfer
- Asset Disposal

### 6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video

### Appendices

- A1: Acceptable Use Agreement (Staff, Volunteers and Governors)
- A2: Acceptable Use Agreement including photo/video permission (Parents)
- A3: Acceptable Use Agreements (Pupils )

## 1. Introduction and Overview

**Rationale:** The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Bishop John Robinson Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

**The main areas of risk for our school community can be summarised as follows:**

### Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

### Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

### Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

## Scope

This policy applies to all members of Bishop John Robinson CofE primary School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Bishop John Robinson CofE primary School IT systems, both in and out of Bishop John Robinson CofE primary School

## Roles and responsibilities

Role	Key Responsibilities
Headteacher	<ul style="list-style-type: none"><li>• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance</li><li>• To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding.</li><li>• To take overall responsibility for online safety provision</li><li>• To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling</li><li>• To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services</li><li>• To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles</li><li>• To be aware of procedures to be followed in the event of a serious online safety incident</li><li>• Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised</li><li>• To receive regular monitoring reports from the Online Safety Co-ordinator</li><li>• To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager</li><li>• To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety</li><li>• To ensure school website includes relevant information.</li></ul>
Online Safety Co-ordinator/Designated Child Protection	<ul style="list-style-type: none"><li>• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents</li><li>• Promote an awareness and commitment to online safety throughout the school community</li></ul>

<b>Role</b>	<b>Key Responsibilities</b>
Lead (This is the same person)	<ul style="list-style-type: none"> <li>• Ensure that online safety education is embedded within the curriculum</li> <li>• Liaise with school technical staff where appropriate</li> <li>• To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs</li> <li>• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident</li> <li>• To ensure that online safety incidents are logged as a safeguarding incident</li> <li>• Facilitate training and advice for all staff</li> <li>• Oversee any pupil surveys / pupil feedback on online safety issues</li> <li>• Liaise with the Local Authority and relevant agencies</li> <li>• Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.</li> </ul>
Governors/Safeguarding governor (including online safety)	<ul style="list-style-type: none"> <li>• To ensure that the school has in place policies and practices to keep the children and staff safe online</li> <li>• To approve the Online Safety Policy and review the effectiveness of the policy</li> <li>• To support the school in encouraging parents and the wider community to become engaged in online safety activities</li> <li>• The role of the online safety Governor will include: regular review with the online safety Co-ordinator.</li> </ul>
Computing Curriculum Leader	<ul style="list-style-type: none"> <li>• To oversee the delivery of the online safety element of the Computing curriculum</li> </ul>
Network Manager/technician	<ul style="list-style-type: none"> <li>• To report online safety related issues that come to their attention, to the Online Safety Coordinator</li> <li>• To manage the school's computer systems, ensuring <ul style="list-style-type: none"> <li>- school password policy is strictly adhered to.</li> <li>- systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date)</li> <li>- access controls/encryption exist to protect personal and sensitive information held on school-owned devices</li> <li>- the school's policy on web filtering is applied and updated on a regular basis</li> </ul> </li> </ul>

Role	Key Responsibilities
	<ul style="list-style-type: none"> <li>• That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant</li> <li>• That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher</li> <li>• To ensure appropriate backup procedures and disaster recovery plans are in place</li> <li>• To keep up-to-date documentation of the school's online security and technical procedures</li> </ul>
Data and Information (Asset Owners) Managers (IAOs)	<ul style="list-style-type: none"> <li>• To ensure that the data they manage is accurate and up-to-date</li> <li>• Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.</li> <li>• The school must be registered with Information Commissioner</li> </ul>
LGfL Nominated contact(s)	<ul style="list-style-type: none"> <li>• To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant</li> </ul>
Teachers	<ul style="list-style-type: none"> <li>• To embed online safety in the curriculum</li> <li>• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)</li> <li>• To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws</li> </ul>
All staff, volunteers and contractors.	<ul style="list-style-type: none"> <li>• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction.</li> <li>• To report any suspected misuse or problem to the online safety coordinator</li> <li>• To maintain an awareness of current online safety issues and guidance e.g. through CPD</li> <li>• To model safe, responsible and professional behaviours in their own use of technology</li> </ul> <p><b>Exit strategy</b></p> <ul style="list-style-type: none"> <li>• At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving</li> </ul>

Role	Key Responsibilities
	<p>PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.</p>
Pupils	<ul style="list-style-type: none"> <li>• Read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy annually</li> <li>• To understand the importance of reporting abuse, misuse or access to inappropriate materials</li> <li>• To know what action to take if they or someone they know feels worried or vulnerable when using online technology</li> <li>• To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school</li> <li>• To contribute to any 'pupil voice' / surveys that gathers information of their online experiences</li> </ul>
Parents/carers	<ul style="list-style-type: none"> <li>• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren</li> <li>• to consult with the school if they have any concerns about their children's use of technology</li> <li>• to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images</li> </ul>
External groups including Parent groups	<ul style="list-style-type: none"> <li>• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school</li> <li>• to support the school in promoting online safety</li> <li>• To model safe, responsible and positive behaviours in their own use of technology.</li> </ul>



**Communication:**

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/Fronter and Google Classroom
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

**Handling Incidents:**

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Online Safety Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

**Handling a sexting / nude selfie incident:**

[UKCCIS "Sexting in schools and colleges"](#) should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people  
*When assessing the risks the following should be considered:*
  - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
  - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
  - Are there any adults involved in the sharing of imagery?
  - What is the impact on the pupils involved?
  - Do the pupils involved have additional vulnerabilities?
  - Does the young person understand consent?
  - Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care

- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

### **Reviewing and Monitoring Online Safety**

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

## **2. Education and Curriculum**

### **Pupil online safety curriculum**

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through the pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

### **Staff and governor training**

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

### **Parent awareness and training**

This school:

- Runs a rolling programme of online safety advice, guidance and training for parents.
- Offers an online safety webpage

### **3. Expected Conduct and Incident management**

#### **Expected conduct**

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

#### **Staff, volunteers and contractors**

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

#### **Parents/Carers**

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

## **Incident Management**

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

## **4. Managing IT and Communication System**

### **Internet access, security (virus protection) and filtering**

This school:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through the LGfL;
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

## Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users - the LGfL USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to [DfE guidance](#);
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the [EU data protection directive](#) where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school's network / We also provide a different/use the same username and password for access to our school's network;
- All pupils have their own unique username and password which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any device loaned to them by the school, is used primarily to support their professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;  
e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:

- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

#### **Password policy**

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
- We require staff to change their passwords into the MIS, LGfL USO admin site, every 90 days/twice a year.
- We require staff using critical systems to use two factor authentication.

#### **E-mail**

##### **This school**

- Provides staff with an email account for their professional use, London Staffmail/LA email and makes clear personal email should be through a separate account;
- We use anonymous or group e-mail addresses, for example [info@schoolname.la.sch.uk](mailto:info@schoolname.la.sch.uk)/[head@schoolname.la.sch.uk](mailto:head@schoolname.la.sch.uk)/or class e-mail addresses.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

**Pupils:**

- We use LGfL pupil email system which are intentionally 'anonymised' for pupil protection.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

**Staff:**

- Staff can only use the LA or LGfL e mail systems on the school system
- Staff will use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

**School website**

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

**Cloud Environments**

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.



## **Social networking**

### **Staff, Volunteers and Contractors**

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- for the use of any school approved social networking will adhere to school's acceptable use policy

### **School staff will ensure that in private use:**

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school /academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

### **Pupils:**

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

### **Parents:**

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

### **CCTV**

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

## 5. Data security: Management Information System access and Data transfer

### Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

### Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to [The Waste Electrical and Electronic Equipment Regulations 2006](#) and/or [The Waste Electrical and Electronic Equipment \(Amendment\) Regulations 2007](#). [Further information](#) can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

## 6. Equipment and Digital Content

### Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.
- Mobile devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets. 'Mobile-free' signs to this effect are displayed.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

## **Storage, Synching and Access**

### **The device is accessed with a school owned account**

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

### **The device is accessed with a personal account**

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

## **Students' use of personal devices**

- The School strongly advises that student mobile phones and devices should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.

## **Staff use of personal devices**

- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own

mobile number for confidentiality purposes and then report the incident with the Headteacher / Designated Officer.

- If a member of staff breaches the school policy then disciplinary action may be taken.

### **Digital images and video**

#### **In this school:**

- We gain parental/carers permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school (or annually).;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

## Appendix 1: Internet permission form

Dear Parents/Carers,

### INTERNET PERMISSION FORM

As part of the school's ICT programme we offer pupils supervised access to the Internet, the global network of computers you will have read about and seen on television. **Before being allowed to use the Internet, all pupils must obtain parental permission and both they and you must sign and return the enclosed form as evidence of your approval and their acceptance of the school rules on this matter.**

Access to the Internet will enable pupils to explore thousands of libraries, databases, and bulletin boards while exchanging messages with other Internet users throughout the world. Families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Whilst our aim for Internet use is to further educational goals and objectives, pupils may find ways to access other materials as well. We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for access.

During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

We would be grateful if you could read the enclosed guidance documents and then complete the permission form that follows.

Yours sincerely,

Mr Ken Maslin  
Headteacher

.....  
**INTERNET PERMISSION FORM - Please complete and return this form to the Headteacher.**

**PUPIL - As a school user of the Internet, I agree to comply with the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the school.**

**Pupils Signature:**.....

**PARENT - As the parent/carer of the pupil signing above, I grant permission for my son or daughter to use electronic mail and the Internet. I understand that pupils will be held accountable for their own actions. I also accept responsibility for setting standards for my son or daughter to follow when selecting, sharing and exploring information and media.**

**Parent/Carer signature:**..... **Dated:** .....

**Telephone Number:** mobile ..... **Home:** .....

**Name of Pupil:** ..... **Year:** .....

## Appendix 2: Acceptable Use Policy

Covers use of all digital technologies in school: i.e. **email, Internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, equipment and systems.**

**Bishop John Robinson CofE Primary School** regularly reviews and updates all AUA documents to ensure that they are consistent with the school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password and change my passwords regularly. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, *or any Local Authority (LA) system I have access to.*
- I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business. This is currently *LGfL StaffMail*
- I will only use the approved *LGfL StaffMail, online cloud storage service – FRONTER and school approved communication systems including TWITTER, GOOGLE CLASSROOM, CLASS DOJO* with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- **I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the head teacher**
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems.*
- **I will ensure that any USB device I use in school is Encrypted**
- **I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils. I will not store any such images or videos at home or on any personal devices.**

- **I will follow the school's policy on use of mobile phones (see below) .Private calls/texts/messages or other communication must be made when away from children.**
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on: Fronter, The school's shared drive, Google Classroom, the school Twitter account, the school website
- **I will only I take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.**
- I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using the *LGfL system* and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert *the Bishop John Robinson's* Child Protection lead / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to *the head teacher*
- I understand that all Internet and network traffic / usage can be logged and this information can be made available *to the Headteacher* on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I will only use any LA system I have access to in accordance with their policies.
- *Staff that have a teaching role only:* I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.







### **Bishop John Robinson Pupil Online Acceptable Use Agreement**

*This agreement will help keep me safe and help me to be fair to others*

- ***I am an online digital learner*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. I only use sites, games and apps that my trusted adults say I can.
- ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
- ***I am careful online*** – I think before I click on links and only download when I know it is safe or has been agreed by trusted adults. I understand that some people might not be who they say they are, so I should be very careful when someone wants to be my friend.
- ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
- ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send photos without checking with a trusted adult.
- ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.
- ***I am a rule-follower online*** – I know that some websites have age restrictions and I respect this; I only visit sites, games and apps that my trusted adults have agreed to.
- ***I am considerate online*** – I do not join in with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.
- ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed or is worried or upset by things they read, watch or hear.
- ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and who with.
- ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
- ***I am SMART online*** – I understand that unless I have met people in real life, I can't be sure who someone is online, so if I want to meet someone for the first time, I must always ask a trusted adult for advice.

- *I am a creative digital learner online* –I get creative to learn and make things! I only edit or delete my own digital work and only use other people's with their permission or where it is copyright free or has a Creative Commons licence.
- *I am a researcher online* – I use safer search tools approved by my trusted adults. I understand that not everything online can be believed, but I know how to check things and know to 'double check' information I find online.

*I have read and understood this agreement. I know who are my trusted adults are and agree to the above.*