Online safety and acceptable use policy

Our Christian Vision

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

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

Safeguarding

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

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety and what is acceptable use, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, '**Keeping Children Safe in Education'** and its advice for schools on:

- Teaching online safety in schools.
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff.
- Relationships and sex education – see section 4.
- Searching, screening and confiscation.

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety.

The governor who oversees online safety is Ruth Oseme.

All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 1).

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding team

Details of the school's DSL and deputy/deputies are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DS team are responsible for online safety in school through:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on 'online safety in school' to the governing board.

3.4 The ICT Technician

The ICT Technician is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 1), and ensuring that pupils follow the school's terms on acceptable use (appendices 2 and 3).

- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Provide appropriate supervision when children are using digital technology for the purposes of remote learning.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 2 and 3).
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
    - What are the issues? - UK Safer Internet Centre
    - Hot topics - Childnet International
    - Parent factsheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 1).

3.8 Use of Microsoft Teams to support Remote Learning

Live streams will be recorded at the start of each session. The teacher leading the live stream will record the session and these will be uploaded and stored on the school network – Remote Learning.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.

- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

- The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website and also a yearly parents' meeting.
- This policy will also be shared with parents.
- Online safety will also be covered during parents' evenings.
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.
- Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but they hand them into the main office for safe keeping. At the end of the school day, pupils can collect their mobile devices from the main office.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school’s ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school’s ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The Safeguarding Team log behaviour and safeguarding issues related to online safety.

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

13. Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy

Behaviour policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

Appendix 1

St Bartholomew's Church of England Primary School

Strawberry Lane, Armley, Leeds LS12 1SF

'Acceptable usage of ICT' policy – Staff/Volunteers

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

This policy is based on the main statements from the school's E-Safety policy concerning members of staff.

All staff are expected to comply with and sign this policy to ensure they are fully aware of their professional responsibilities when using any form of information & communication technology.

Any concerns, or clarification needed on the contents of this policy, should be discussed with the Head Teacher, E-Safety Coordinator or ICT Technician.

A company called 'Talk Straight' are quoted in this policy. They were known previously as 'Schools Broadband' and they are responsible for the school's internet connection as well as the school's filtering system. There is a small piece of software on all laptops that detects whether a user is a pupil or staff when they logon. Appropriate filtering is applied to all laptops which dictates what content a user is allowed to view when browsing the internet.

I understand that

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

I will

- Comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- Only use the school's ICT systems (including hardware, software, email, Internet, Intranet, Learning Platform) and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or the Governing Body.

- Ensure that all electronic communications with pupils, parents and staff are compatible with my professional role.

(continued overleaf)

- Take all reasonable steps to ensure that school data is stored securely and used appropriately in school, off school premises, or accessed remotely.
- Respect copyright and intellectual property rights.
- Support and promote the school's E-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- Report any accidental misuse of school ICT, or accidental access to inappropriate material, to the E-Safety Coordinator, Head Teacher or ICT Technician.
- Immediately inform the ICT Technician if I receive any offensive e-mail.
- Report any incidents of concern regarding children's safe use of ICT to the E-Safety Coordinator, Child Protection Designated Lead, Head Teacher or ICT Technician.

I will not

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

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

Signature ……………………………………………………….

Date ……………………………………………………….

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

Laws which may apply: Computer Misuse Act 1990, Data Protection Act 1998, Communications Act 2003, Copyright Design and Patents Act 1988, Malicious Communications Act 1988, Obscene Publications Act 1959 and 1964, Racial and Religious Hatred Act 2006, Sexual Offences Act 2003, The Telecommunications (Lawful Business Practice -Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Protection from Harassment Act 1997, Public Order Act 1986, Human Rights Act 1998, Protection of Children Act 1978, (EU) 2016/679 (General Data Protection Regulation)

St Bartholomew's C of E Primary School

Appendix 2

Code of Conduct for the Acceptable Use of ICT
Year 1 and Year 2 Pupils

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

This is part of my learning about E-Safety.

I understand that

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

I will

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

I will not

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

Full name ……………………………………………………………..….

Class ……………………….……………………………………..….

Date ………………….……..

Year 2 will normally complete this during September.

Year 1 pupils will complete this sometime during the year, whenever their teacher considers that they understand the rules.

St Bartholomew's C of E Primary School

Appendix 3

Code of Conduct for the Acceptable Use of ICT

Year 3, Year 4, Year 5 and Year 6 Pupils

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

This is part of my learning about E-Safety.

I understand that

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

I will

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

(continued)

I will not

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

I agree to obey this code of conduct

Signature ……………………………………………………………..…

Class ……………………………………………………………..…

Date ………………………………………………………………

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