

ONLINE SAFETY POLICY

Bishop Ellis Catholic Primary School




Our Mission

I have come in order that you may have life—life in all its fullness (John 10:10).

We Love, We Pray, We Learn, We Play.

Values: Love God; Aspire to be your best; Be honest; Forgive; Care

Approved by: FGB	Date: July 2020
Signed: 	
Last reviewed: 19.6.20	
Scheduled date of next review: June 2022	

Contents

1. Introduction and aims	2
2. Legislation and guidance	2
3. Roles and responsibilities	3
4. Educating pupils about online safety	5
5. Educating parents about online safety	5
6. Cyber-bullying	6
7. Acceptable use of the internet in school	6
8. Pupils using mobile devices in school	7
9. Staff using work devices outside school	7
10. How the school will respond to issues of misuse	7
11. Training	8
12. Monitoring arrangements	8
13. Links with other policies	8
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)	9
Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)	10
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)	11

1. Introduction and Aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

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](#)

› [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 logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Mrs Erin O'Hagan (Chair of Governors)

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 3)

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 lead and deputies

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

The DSL, and deputies, take lead responsibility for online safety in school, in particular:

- › ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- › Working with all 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. A tailored self-audit document can be used to identify gaps in knowledge to ensure that the training is purposeful and effective.
- › Liaising with other agencies and/or external services if necessary
- › Providing regular reports on online safety in school to the governing board

This list is not intended to be exhaustive.

3.4 ICT management

Bishop Ellis Catholic Primary School understands it relies on partnerships with specialist ICT companies (Arkel, RM & Capita) to support it with:

- › 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 regular basis.
- › Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- › Working with the DSL and DDSL 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

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- › Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- › Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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 3).

Initial Teacher Training (ITT) students completing long term placements within the school, will be made aware of this policy and are expected to agree to terms of Acceptable Use (appendix 3) prior to starting their placement as part of their induction to Bishop Ellis.

4. Educating pupils about online safety

As a Catholic school, we encourage children to live out the school's values 'aspiring to be our best' and 'being honest' when using technology to communicate and work online both in school and at home. We aim to embed these values and the school's ethos into lessons involving internet safety and when discussing appropriate internet usage.

Our school recognises that the internet and other digital technologies can transform learning; helping to improve the outcomes for children and young people; promote creativity; all of which add up to a more exciting and challenging classroom experience. The internet gives us opportunities to 'live life in all its fullness' (John 10:10) as long as children are taught to be aware and careful where online safety is concerned.

To this end, Bishop Ellis will enable pupils to exercise the skills of critical awareness, digital literacy and good online citizenship. 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.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and through information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings and through an annual 'e-safety' parents' meeting for Upper Key Stage 2.

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/DDSL.

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. Teachers will discuss cyber-bullying with their class, 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 provides information on cyber-bullying, via the school's website, to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. The school's website also offers support to parents to help keep their child safe online.

In relation to a specific incident of cyber-bullying and/ or misuse of the Internet, in line with the school behaviour policy, this may result in the exclusion from using the Internet or the school's virtual learning websites for a fixed term period. Parents will be informed of this. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained and the children's wellbeing is prioritised.

Incidents of cyber-bullying or misuse outside of school between Bishop Ellis pupils, which are made known to school will be dealt with accordingly and in line with the school's behaviour policy as stated above. When an incident occurs and school is made aware, a log will be kept of this and reminders of appropriate internet use in class will occur in a timely manner. (see section 4 for ways we teach online safety at Bishop Ellis)

The DSL/DDSL will consider whether any 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.

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

Upper Key Stage 2 pupils may bring mobile devices into school, if this has been requested by parents and authorised by school. Pupils are not permitted to use them during the school day. Mobile phones must be left in the school office, where they will be kept safe. Mobile phones can be collected by pupils at the end of the day and are not to be used on the school site.

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 3.

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.

The use of Google Drive to store data is password encrypted and staff must ensure their password is not shared. Staff are to ensure that confidential information is kept in their 'personal drive' as opposed to 'shared drives'. For the purpose of GDPR any personal information relating to the children should be kept secure in the Google Drive or on an encrypted memory stick.

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

Work devices must be used solely for work activities, in line with the iPad/ laptop loan agreement document which will be signed by all staff with a school laptop and iPad, when received, as part of their induction.

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 behaviour policy, whereby a fixed term exclusion from internet/ virtual learning websites may be enforced for a fixed term. 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 code of conduct, whereby disciplinary action may be taken, but not limited to dismissal. 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.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material, *will* be reported to the police:

- Images of child abuse (images of children whether they be digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative).
- Adult materials that potentially breaches the Obscene Publications Act (1959) in the UK.
- Criminally racist or anti-religious material
- Violence and weapon making ('Prevent' agenda)
- Illegal taking or promotion of drugs
- Software piracy
- Other criminal activity

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. They will be required to read this policy and agree to the terms of acceptable internet usage. (see appendices)

All staff members will receive refresher training annually, as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings). Staff will annually be required to read this policy and agree to the terms of acceptable internet usage. (at the beginning of each academic year so to include new staff)

The DSL and DDSL 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, 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 DSL and DDSL log behaviour and safeguarding issues related to online safety.

This policy will be reviewed every 2 years by the Governing Body. At every review, the policy will be shared with all staff, governors, volunteers and visitors as necessary.

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: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

(reviewed annually at the start of a new academic year)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher **immediately** if:
 - I click on a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers & other devices for schoolwork only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it.

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:



Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

(reviewed annually at the start of a new academic year)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Use any inappropriate language when communicating online
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I need to bring a personal mobile phone into school:

- My parent will make a request through the school office and school will authorise whether I can bring my device with me.
- I will ensure that it is kept in the office during the school day, where I know it will be safe.
- I will take responsibility for collecting my mobile phone at the end of the school day and not use my phone on the school site unless I have special permission from a member of school staff.

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:



Appendix 3: Acceptable Use Agreement (staff, governors, ITT students, volunteers and visitors)

(reviewed annually at the start of a new academic year)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first (if you are not their class teacher)
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices, including external memory, are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the iPad/laptop loan agreement.

I will let the designated safeguarding lead (DSL) know if a pupil informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

