



IT & E-Safety Policy

Mission Statement

Botwell House Catholic Primary School is distinguished by the care, courtesy and concern extended to all its members, regardless of cultural differences and strives to follow the teachings of Jesus Christ to:

“Love one another as I have loved you”

Through an effective partnership between home, school and parish and through a broad and balanced curriculum, each valued individual is encouraged to grow in their journey of faith and strive towards excellence.

Botwell House Catholic Primary School seeks to ensure that all pupils receive a full-time education which maximises opportunities for each pupil to realise his/her potential.

Current revision:	<u>07.07.26</u>
Date for further revision:	<u>07.07.28</u>
Delegated to:	HT
Reviewer:	K. Oakley

Contents

1. Definitions:	3
2. Policy Statement	4
3. Overview:	4
4. Implementing the Policy:	4
5. Using the Internet in school:	5
6. Managing Systems:	6
7. Emails:	7
8. Cyber-bullying:	7
9. Publishing content and the School Website:	8
10. Mobile Phones:	8
11. Digital images:	9
12. Social Networking:	10
13. Filtering:	11
14. Handling e-safety complaints:	11
15. Data Protection Act:	11
16. Staff and Pupil Agreements:	12

Definitions:

Acceptable use: A policy that a user must agree to abide by (AUP) in order to gain access to a network or the internet. It may also cover how other communications devices, such as mobile phones and camera phones, can be used on the premises.

Cookie: a piece of data stored in your computer after you have visited a website, that allows the web page to be downloaded faster.

Digital video: Video captured, manipulated and stored in a digital format.

Filtering: A method used to prevent or block users' access to unsuitable material on the internet.

Firewall: A network security system used to restrict external and internal traffic.

Hacking: The process of illegally breaking into someone else's computer system breaching the computer's security.

Internet service provider (ISP): A company providing a connection to the internet and other services, such as browser software, email, a helpline, web space and subscriber-only content.

Instant messaging (IM): Allows users to communicate with other users, providing an easy way of sending short written messages to a few friends online at the same time. It includes text messaging, voice chat, webcams, and file and picture exchange.

Spam: Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones.

Spoofing: Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

Virus: A computer programme which enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.

Webcam: A webcam is a camera connected to a computer that is connected to the internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.

Policy Statement:

This policy applies to all members of the Botwell House Catholic Primary School community (including staff, children, governors, volunteers, parents / carers and visitors,) who have access to and are users of school IT systems, both in and out of school. The policy demonstrates the safeguards in place to help ensure, as far as reasonably practicable, that the risks associated with IT and electronic communications are considered and controlled.

Overview:

Botwell House Catholic Primary School recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that pupils, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

E-safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility and as a result we endorse a whole school approach involving all stakeholders.

Implementing the Policy:

This policy is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during RSE lessons where personal safety, responsibility, and/or development are being discussed.

Using the Internet in School:

At Botwell House, the internet is used to raise educational standard; to promote pupil achievement; to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

Some of the benefits of using ICT and the internet in schools are:

For children:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.

Staff will ensure that:

- In lessons where internet use is pre-planned, children are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches. Staff will guide pupils in online activities that will support learning outcomes planned for the pupils' age and maturity.
- Where children are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the children visit.
- Children are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information.

- Children are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Managing Systems:

Botwell House School is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by INFRATEK Ltd and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- All users need to log on using a username and password. Children log on using individual/year group login and password. *Children are taught that they should only access the network using that particular log in.* **We expect all users to only login using their username.**
- Each user is given an allocation of disk space for the storage of their work. *Children are taught how to save their work into their “My documents” area.* **We expect children to save and keep their work to build up a portfolio of evidence.**
- On the network there are “shared resource” areas where many different groups of users can save work so that it is available to others. *Children are taught how to access and save to these shared resource areas.* **We expect all users to respect the contributions of others, not to delete or alter others’ work and to ensure that they only save work to shared areas with permission.**
- All users are taught to only print when necessary to save resources for financial and environmental reasons. **We expect children to only print out work when directed by staff to do so.**
- Antivirus software has been installed and configured for the laptops/computers and will automatically download from internet connection. **No user interaction is required**
- Only the network administrators are permitted to install software on to computers. **We expect all users to make no attempt to load or download any programme onto the network.**
- All users of the network can be monitored remotely by the network administrators. *Children are taught that their use of the network can be monitored.* **We expect all users to understand that their use is subject to monitoring.**
- Consent of the IT Department is required to adjust or alter the laptops/computers by the addition or deletion of any hardware.
- All teaching staff have school laptops. School data, including emails, shall not be stored, shared or transmitted to private accounts.
- It is the staff responsibility to clean/update and delete files not in use at the end of every year. The ‘My documents’ file must only store information needed for the next year and must not hold duplicate files.

For more information on data protection in school please refer to our **data protection policy** on the school website.

Emails:

Botwell House School uses email internally for staff, and externally for contacting parents, external agencies and schools; is an essential part of school communication. Staff and pupils should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact other members of staff and other professionals for work purposes. This is important for confidentiality.

Staff should be aware of the following when using email in school:

- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell their line-manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

Cyber-bullying:

Cyberbullying, as with any other form of bullying, is taken very seriously by our school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the **behaviour policy**. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does come up, the school will:

- take it seriously
- act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- record and report the incident on CPOMs
- provide support and reassurance to the victim
- make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or

emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a consequence is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. This will be done in collaboration with the parents of the child. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in school.

Publishing content and the School Website:

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, children, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the school will be for the school office only.

Mobile Phones:

While mobile phones and personal communication devices are common place in today's society, their use and the responsibility for using them should not be taken lightly.

- The school accepts that staff will bring their phones to work.
- Staff mobiles must be kept switched off or on silent at all times and not looked at, handled or answered during lessons, meetings or anywhere accessible by the children.
- On occasions the Headteacher will authorise staff to keep the phone on their person due to extenuating personal circumstances. The individual should still, when the phone vibrates (ringer should still be off), quickly find a place where no children are accessing prior to answering the call. Without this specific dispensation from the HT, Staff must not leave the classroom during lessons to use their mobile phones. Mobile phones should only be used during break times and lunch in office areas that children cannot access at this time. Any member of staff using a mobile phone without permission may be subject to action in line with the school's disciplinary policy.

- Mobile phones should not be used in a space where children are present.
- Staff are not permitted to use recording equipment on their mobile phones, for example: to take photographs or videos of children.
- Staff are not to give their home or mobile telephone number to children or families.
- Staff should not communicate electronically with children from school other than via school approved software ie. Microsoft Teams to discuss home learning content or as part of a curricular planned activity. In this instance it would be from and to @botwellhouse.school email addresses and SLT will be fully aware of the instance.
- Staff should not enter into instant messaging communications with children.
- Only Year 6 children who travel to/from school alone are permitted to have mobile phones in school from the start of the summer term to support their transition and develop independence ready for secondary school. Children's phones are to be handed to staff in line with the Mobile Phone Policy. **No other children are permitted to carry a mobile phone in school and parents will be contacted if one is found**
- The sending of abusive or inappropriate text messages or photos is forbidden

It is important to note that the school provides mobile phones for Senior Leaders. These phones are the property of the school and are used for a great number of functions such as alerts for behavioural incidents and safeguarding concerns by staff. It is important that the school is transparent that these people do use these phones on site as part of their specific role.

Smart watches and trackers

Smart watches and physical activity trackers are common place now. Children are only allowed to have activity trackers that have no internet/camera capacity. Smart watches are not allowed for children at all. Staff on the other hand can have their smartwatches but Bluetooth capability must be off when in school and no other functions are to be used other than to tell the time. Failure to follow the aforementioned will lead to disciplinary action in line with policy.

Digital Images

- Digital still and video cameras are used for recording special events as well as being essential tools for everyday learning experiences across the curriculum. As part of our GDPR policy, all parents/carers are asked to sign consent forms to allow pictures/videos of their children to be posted on the school website, classroom DOJO or Twitter account. Some images celebrating the work of children involved in everyday and special event activities may be selected to be shown on the school website. A child's full name with their image will never be posted on any school site. **The school will happily remove any image of a child on the school website at their parent's request.**
- Digital images may be shared with partner schools and organisations as part of collaborative learning projects. This can include live video conferencing. All such use

is monitored and supervised by staff. *All users are taught to seek permission before copying, moving, deleting or sending any images taken within school. We expect all users to seek permission from the Head teacher before sharing images outside of the school environment.*

- Staff may take digital images using school equipment (Cameras, ipads and visualisers)
- At the end of every year all photos are to be stored on the photo drive under the pupil's year of entry. It is the staff's responsibility to select appropriate photos to be saved at the end of every year for their final year book. Year 6 delete all photos after the year book has been created.
- Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- At Botwell House we do allow parents to take video and photographs at school events. **However, we do ask parents to respect privacy and so photography at events is on the understanding that photographs that contain images of children other than their own will not be posted anywhere on the internet.**

Social Networking

- The school will block/filter access to social networking sites and newsgroups unless a specific use is approved
- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils are advised not to place personal photos on any social network space.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils are encouraged to invite known friends only and deny access to others.
- Pupils and parents are made aware that some social networks are not appropriate for children of primary school age and the legal age to hold accounts on many such as YouTube or Instagram is 13 years old.

Filtering

The school will work in partnership with School's Broadband to ensure filtering systems are as effective as possible.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and their risks assessed.
- **Podcasting** – Some children will be given opportunities to create oral recordings. Some of these recordings may be made available as podcasts through the Internet so that they can be shared with interested members of the school community.

Published Content & The School Website

- The contact details on the web site should be the school address, email and telephone number. Staff or pupil's personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate

Copyright

Though there are lots of free to use resources on the Internet, the majority of image, sound and music files are covered by copyright laws. Some can be used for educational reasons without permission provided that the source is stated and that they are not made available outside the school. Some cannot be used under any circumstances; this is particularly so for music but can apply to other types of file e.g. photographic images. Care therefore needs to be taken with multi-media work which incorporates anything downloaded from the Internet or any other published source that it is not uploaded onto the school's website or broadcast through any other technology. *Children are taught that the people who put their work on the Internet may not always want people to copy or use their work and that they should check whether they have permission.* **We expect all users to respect copyright laws.**

- It is important to know what work is original and when chunks of text have been copied from other sources such as the Internet. *Children are taught that they should not present the work of others as their own work. Older children are taught about copyright and how to extract or paraphrase information.* **We expect all children to make it clear what is their own work and what is quoted from other sources.**

Handling E-Safety Complaints

- Complaints of internet misuse will be dealt with in line with the complaint Policy that the school has adopted.
- Any complaint about staff misuse must be referred to the head teacher and will be dealt with under the allegations against staff policy potentially. These will be logged and dealt with as deemed appropriate by the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.

Data Protection Act

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Staff and Pupil agreements



Staff & Governor Agreement

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Headteacher (for staff,) and Chair of Governors (for governors).
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. 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 / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure Outlook email system for any school business.
- I will delete all emails that are over 2 years old at the start of every academic year.
- I will only use the approved school email, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to Mrs Helen Slater.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet 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, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- 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 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 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 will embed the school's e-safety curriculum into my teaching.

- I (Staff only) will alert the Safeguarding team via CPOMS if I feel the behaviour of any child I teach may be a cause for concern.

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

SignatureDate.....

Full Name (printed)

Job title

The following agreement needs to be signed by the children when being inducted into year 3 (start of KS2,) and then revisited at the start of each of the following years to remind the children and staff.

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carers has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.

I have read and understand these rules and agree to them.

Signed:

Date:

KS1 Pupil Acceptable Use Agreement

Think before you click

S



I will only use the Internet and email with an adult

A



I will only click on icons and links when I know they are safe

F



I will only send friendly and polite messages

E



If I see something I don't like on a screen, I will always tell an adult

My Name:

My Class