The Bishop Wheeler Catholic Academy Trust

Policy

ICT Acceptable Use

Published: May 2026

To be reviewed: 2029/30

The Bishop Wheeler Catholic Academy Trust

Our Mission

Outstanding Catholic education for all pupils. As a family of schools, we will enable our young people to develop spiritually, morally, intellectually and personally, putting their faith into action, through serving Christ in others, in the church and in the world around them.

This policy was approved by the Chief Executive Officer on behalf of the Trust Board

Signature:

Mr D Beardsley
Chief Executive Officer

Date: 15/05/2026

Version History

Version		4.0	
Date		15/06/26	
Approved by Chief Executive Officer		15/06/26	
Version	**Date**	**Description**	**Revision Author/s**
1.0 Published	July 2021	Trust Policy	GNE/DBY/JJN
2.0 Review	September 2021	Trust Policy Review	JJN/DBY/NFR
3.0 Review	October 2023	Trust Policy Review	SCK/NFR/JJN/DBY
4.0 Review	April 2026	Trust Policy Review	JJN/DBY/NFR/SCK

Change review

Version	Date	Changes
1.0	July 2021	New Policy
2.0	September 2021	**USB** – Information updated
3.0	September 2023	**Definitions –** Information updated **Introduction –** Information updated **Privacy –** Information updated **IT Manger** - Information updated **Management of the policy** – Information updated **Inventory –** Information updated **Printing –** Information updated **E-mail –** Information updated
4.0	May 2026	**Page 5 –** Definitions updated **Page7 –** Introduction updated **Page 7** – Purpose updated **Page 9** – Personal Devices added **Page 14 and 15-** Update to ICT agreement for pupils

ICT Acceptable Use Policy

Contents

Definitions

In this policy for ICT Acceptable Use, unless the context otherwise requires, the following expressions shall have the following meanings:

BWCAT	The Bishop Wheeler Catholic Academy Trust.
Trust, we and our	Covers all of the schools within The Bishop Wheeler Catholic Academy Trust and The Bishop Wheeler Catholic Academy Trust Office.
Child and Children	Refer to children and young people under the age of 18 years.
BWCAT Trust Board	The Directors of the Trust Board.
Academy Council	Governors elected or appointed to individual Academy Councils.
Governors	Governors appointed to the Academy Council of the individual academy.
CEO	The Chief Executive Officer for the Trust.
Executive Headteacher/Headteacher	Executive Headteacher/Headteacher responsible for individual academies.
Academy/schools	The Academies within BWCAT.
Pupil	Any pupil on roll at any of the BWCAT schools.
Parents	Any person who holds parental responsibility for the pupil.
Staff	Means all employees, temporary, casual, agency and contracted staff working for the Trust, volunteers and consultants.
DPO	Data Protection Officer
Managed Service Provider	A third-party business that provides ICT services.
Lead Person	CEO for the Central team and Executive Headteacher/Headteacher for individual academies.
ICT	Information and Communication Technologies.

MFA	Multi Factor Authentication, which is used as an additional security layer to protect Trust data.
Electronic Devices	Includes, but not limited to laptops, desktop computers, mobile phones, iPods, iPads, smart watches, cameras, printers, televisions, DVD players and any other device which is capable of storing, displaying, receiving or transmitting data.
Cloud	ICT system not hosted within the Trusts private premises.
ICT Systems	Digital system used to manipulate, store, retrieve or display data and the people who use them.

Introduction

The Bishop Wheeler Catholic Academy Trust recognises the use of its ICT and communications facilities as an important resource for teaching, learning, personal development and as an essential aid to business efficiency.

We are managing a significant investment in the use of ICT. In many areas of work, the use of ICT is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity, stability and security of the ICT systems and data are maintained at a level that is appropriate for our business needs.

All persons involved with the use of any BWCAT ICT systems and devices should be aware of their duties and responsibilities by adhering to these guidelines. Sufficient resources should be allocated each year to ensure the security of the Trust's ICT systems. If there are insufficient resources to fully implement this policy, then the potential risks must be documented and reported to the CEO.

Purpose

This policy is intended to ensure ICT facilities and equipment are dealt with correctly. The use of the latest technology is actively encouraged at BWCAT. With this comes responsibility to protect users, individual schools, and the Trust from abuse or misuse of the system.

All staff and pupils are expected to behave responsibly on the school computer network and with ICT equipment. Failure to comply with this policy may result in disciplinary action.

Located at the end of this document are ICT Acceptable Use Forms (separate form for staff and pupils) that should be signed by every staff member and pupil within the Trust. A record must be retained that the ICT Acceptable Use Form has been signed by all staff and pupils (parents to sign for pupils in Key Stage 1 and 2). The form only needs to be signed once and will remain with the pupil/staff member until they leave the school, if any changes are made to the form during a review of the policy the new form will need to be signed and retained. If a new staff member or pupil attends school during the school year it will be the responsibility of the Lead Person to ensure this policy is provided and the form is signed. Academies must have a record that staff and pupils have read the acceptable use forms and acknowledge they have accepted it, for example this can be completed through google forms or other digital records.

Privacy

In order to protect our staff, pupils and the Trust itself from any third-party claims or legal action, the Trust may view any data, information or material on the Trust's ICT system. (Whether contained in an e-mail, on the network, "cloud" storage, or laptops) and in certain

circumstances, disclose that data to third parties, such as the police or social services, pending official request for data.

Authorisation must first be obtained from the Lead Person to view any data outlined above.

Roles and responsibilities

BWCAT Trust Board

The Trust Board has overall responsibility for ensuring that all schools comply with the guidance in this policy.

Lead Person

The Lead Person is responsible for ensuring that the guidance from this policy is followed by all staff and pupils. They are also responsible for ensuring that any special ICT security measures relating to the school's ICT facilities are applied and documented as an integral part of the policy.

The Lead Person is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the policy and to ensure that the appropriate controls are in place for staff and pupils to comply with the policy. This is particularly important with the increased use of computers and laptops at home. Staff should exercise extreme care in the use of personal data at home to ensure legislation is not contravened, in particular the Data Protection Act 2018/UK GDPR.

IT Manager

For schools where the Trust outsources their IT support to a third-party managed service provider, this policy should be made available to the relevant service provider. It will be the Lead Person's responsibility to ensure the service provider understands and abides by this policy.

Where the school has in house IT support and an IT Manager, they will also be required to follow the guidelines of this policy.

The IT Manager is responsible for both the school's physical and digital ICT infrastructure and will have direct control over these assets and their use, including responsibility for controlling access to these assets and for defining and documenting the requisite level of protection.

The IT Manager will be the official point of contact for ICT security issues within the relative school. The IT Manager will be responsible for informing the Lead Person of

any suspected or actual breach of ICT Security occurring within the school. At schools with a managed service provider, the service provider will make the Lead Person aware of any security issues or breach of ICT security occurring within the school.

The Lead Person should document any suspected or actual breach of ICT systems. The Trust Head of Governance should also be informed so the incident can be reported to the ICO if required.

Users

All users of the school's ICT systems must comply with the requirements of this ICT Acceptable Use Policy. The relevant rules of which each user must abide by and agree to are documented in **Appendix A** for KS1 and KS2 pupils, **Appendix B** for KS3, KS4 and KS5 pupils and **Appendix C** for staff.

All Users have a responsibility to notify the Lead Person of any suspected or actual breach of ICT security. **Appendix D** is the Data Breach Form that should be completed and passed to the BWCAT Head of Governance.

Personal Devices

Staff, pupils, volunteers and parents must not use any personal device (including mobile phones, tablets, smart watches or any device capable of recording audio or video) to record, photograph, livestream or capture audio/video of any other person without their explicit consent. This includes any use on school premises, during school activities, or when representing the Trust. Any breach will be treated as a safeguarding and disciplinary matter.

Management of the policy

1. Suitable training for all ICT users and documentation to promote the proper use of ICT systems will be provided by individual academies. Users will also be given adequate information on the policies, procedures and facilities to help safeguard these systems and related data.

2. In addition, users will be made aware of the value and importance of such ICT systems and data, particularly data of a confidential or sensitive nature and be made aware of their personal responsibilities for ICT security.

3. The Lead Person must ensure that adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures should be applied that provide for continuity of ICT security when

staff vacate or occupy a post, including handover documentation and in the case of the IT Manager / ICT Support a list of passwords and accounts kept securely on the premises and in a digital vault for redundancy purposes.

4. The Lead Person is to record that new staff and pupils have been issued with, have read the appropriate documentation relating to ICT security, and have either signed the list of rules in **Appendix A, B, and C.** Or schools have a record that staff and pupils have read the acceptable use policy and acknowledge they have accepted it, for example through google forms.

5. The Lead Person to record that those rights have been amended or withdrawn due to a change to responsibilities or termination of employment or for a pupil who has left the school.

Location Access

Adequate consideration should be given to the physical security of rooms containing ICT equipment. As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data. The server rooms should be locked when left unattended.

The IT Manager or school's ICT support must ensure appropriate arrangements are applied for the removal of any ICT equipment from its normal location.

Equipment Siting

Reasonable care must be taken in the siting of computer screens, keyboards, printers, or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:

1. Devices are positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved.

2. Equipment is sited to avoid environmental damage from causes such as dust and heat.

3. Users have been instructed to avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained. They should be either locked or the user logged-off. Clear written instructions to this effect should be given to users.

4. Users have been instructed not to leave hard copies of sensitive data unattended on desk.

5. Screens on computers must lock automatically after 30 minutes.

The same rules apply to official equipment in use at a user's home, for example remote working and accessing the school's software remotely.

Printing

As a Trust we continually try to reduce the cost and negative environmental impact of printing. As such wherever possible the number of printers in school will be reduced and access to shared multi-function devices provided as a more sustainable alternative.

Where possible staff should use alternative file sharing systems such as email, OneDrive, and SharePoint. The school printing facilities are not to be used to print personal or non-work-related materials.

All printers should be password protected or accessible via logged secure user login when used for photocopying. Staff should report any problems, such as a paper jam to the school office/IT helpdesk. The problem must not be left, documents that are jammed must be removed from the machine and disposed of securely. Documents must not be left on/in the machine at any time.

The Internet

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and the age of pupils.

Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils age and maturity.

Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location and retrieval.

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils will be educated to understand that unscrupulous individuals and groups may use the internet to undermine their safety

and propagate unacceptable ideas, such as political extremism and intolerant and illegal attitudes.

Pupils will be taught to acknowledge the source of information and to respect copyright when using internet material in their own work.

Appropriate filters and monitoring systems are in place which involve review and reporting of all user's activities on the internet to comply with safeguarding and the Prevent duty.

Risk Assessment

Although there is useful information on the internet, there is a great deal more material which is misleading or irrelevant. Using the internet effectively requires training and self-discipline. Unfortunately, the internet contains a great deal of unsuitable and offensive material. It is important for legal reasons, reasons of principle and to protect the Trusts staff, volunteers and pupils that access to the internet is properly managed. Accessing certain websites and services and viewing, copying, or changing certain material, could amount to a criminal offence and give rise to legal liabilities.

Access Management

All Internet access will be monitored.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the IT Manager/ICT Support. (IT Manager/ICT Support must update the Lead Person).

The IT Manager/ICT support will ensure that regular checks are made to ensure that the filtering methods selected are appropriate.

Any material that the Trust believes is illegal must be referred to the appropriate authorities.

Chat rooms, Social Networking and newsgroups.

Pupils and staff are not allowed to access public or unregulated chat rooms.

Pupils and staff are not allowed to access their own personal social media accounts from school devices unless authorisation has been granted by the Lead Person. Access is granted to school social media sites such as Twitter.

Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.

E-mail

All users who are provided with an e-mail account should only use their email address for educational or business use. Personal or inappropriate use of this resource is strictly prohibited.

The Trust's e-mail disclaimer should be automatically attached to all outgoing e-mails.

The frequency and content of incoming and outgoing external e-mails are checked from time to time. This is to determine whether the e-mail system is being used in accordance with this policy.

Individual e-mail accounts must not be used by any other individual.

Authorisation from the Lead Person must be sought before any email accounts are accessed.

The Lead Person will then decide which senior members of staff are entitled to have read-only access to your e-mails. E-mails constitute records of the Trust and are subject to the same rules, care and checks as other written communications.

Sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing, malicious, threatening, or contravening discrimination legislation will not be tolerated. All incidents must be brought to the attention of the Lead Person for consideration of disciplinary action.

All users should ensure that confidential emails are suitably protected at all times. The IT manager/ICT support can offer guidance on how to send confidential e-mails. For example, through Microsoft 365 email encryption.

Information stored on Trust computer systems.

All users are personally responsible for anything they store on Trust computer systems. Any personal storage media or cloud storage they access from within the Trust. Storage or distribution of offensive material will result in disciplinary action.

The Trust reserves the right to monitor the content of all files stored on its systems. Staff who operate monitoring procedures must seek authorisation from the Lead Person.

Remote Access

Some schools possess a remote access system which allows many concurrent connections for staff working outside the school site (e.g. at home) and helps with flexible working and efficiency savings as well as staff wellbeing.

Any remote access to school systems brings a risk of others not associated with the Trust having visibility of confidential data. The most obvious example of confidential data being accessed is staff using the school's Management Information System (i.e. Arbor) remotely.

Staff will connect remotely to the school systems and have access to the same data and applications they do as if they were in school. This level of access is governed by permissions granted to them based on their job role (for example HR staff will have access to HR records whereas a teacher would not).

Any school issued device used to connect to the remote access system will be subject to the school's ICT security procedures and must not be used by any other individual except the staff member to whom it is assigned.

Trust devices should be kept safe at all times, do not leave devices in vehicles overnight.

All staff will be provided with training before remote access is granted. Staff must not store personal data on Trust devices.

Where a user accesses Trust systems remotely using a personal device, they will still be required to adhere to the Trusts Acceptable Use Policy. The personal device will require MFA to securely access such resources.

Removable Media

There is a danger of exposing the Trust's network to viruses or passing viruses to a third party, via material downloaded from or received via the internet, or brought into the Trust on disk or other storage media.

USB devices carry a high risk of data being lost/stolen. The risk of viruses being passed to our school servers is also high.

USB storage devices must not be used. Alternative systems should be used such as the schools SharePoint, OneDrive or remote system.

It will be the responsibility of the Lead Person to ensure their staff and pupils are not using USB storage devices.

Communication of this Policy

Staff

All staff will be provided with this document and its importance explained. The process of logging onto the trust computer systems will include an agreement to abide by this policy. (**Appendix C**)

Pupils

Rules for reasonable computer use should be posted near all computer systems. Pupils will be informed that computers will be monitored. Instruction and reasonable and safe use should be given to pupils by staff. The process of logging on to the Trust computer systems will include agreement to abide by this policy. (**Appendix A and B)**

Parents

Parents' attention will be drawn to this policy in newsletters and on the Trust/school websites. A partnership approach with parents is encouraged. This will include demonstrations, practical sessions and suggestions for online safety at home.

Appendix A

ICT Acceptable Use Agreement – KS1/KS2 Pupils

I agree that I will:

- Only open pages which my teacher says are ok.
- Tell my teacher if anything makes me feel scared or uncomfortable.
- Make sure all messages I send are polite.
- Show my teacher if I get a nasty message.
- Not replying to any nasty messages or anything which makes me feel uncomfortable.
- Talk to my teacher before using anything on the internet.
- Not play games (unless told to by my teacher) during lesson time.
- Not to tell people about myself online (I will not tell them my name, anything about my family and home, my phone number)
- Not load photos of myself onto the computer.
- Never agree to meet a stranger.
- Not record any teachers or pupils with a phone or watch without them knowing.

I know that anything I do on the computer may be seen by someone else.

Name of child _____ Year_____

I have discussed these rules with my child, and they understand what is expected from them and know what to do when there is an issue.

Name _____

Signed _____

Date _____

Appendix B

ICT Acceptable Use Agreement - KS3/KS4/KS5 Pupils.

This Acceptable Use Agreement is intended to ensure that young people will be responsible and stay safe whilst using school ICT systems and the Internet.

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I will only access the school network through my authorised username and password. I will not use the password of others.
- I understand that the school will monitor my use of the systems, devices, and digital communications.
- I will not use the school IT systems/devices for personal or recreational use, for accessing social media sites, on-line gaming, gambling, internet shopping, file sharing or video broadcasting.
- I will not upload, download, or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not use any programs or software that might allow me to bypass the filtering and security systems in place.
- I will not install programs on any school computer or try to alter school settings.
- I will not use my personal devices (e.g. mobile phone/iPad) in school without permission from the Lead Person. The school accepts no responsibility for any devices brought into school.
- I will not use any personal device to record audio or video of other students or adults without their explicit consent.
- I will carefully write e-mail and other on-line messages making sure the language I use is not strong, aggressive, or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet “on-line friends”.
- I will not take or distribute images of anyone else without the permission of the teacher and the permission of the person(s) in the image.
- I will not take or distribute images of myself or anyone else semi-naked or naked.
- I will not access or use chat and social networking sites whilst at school.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I understand that I am responsible for my actions, both in and out of school.
- I understand that the school has the right to take action against me if I am out of school and where they involve my membership of the school community. (Examples would be cyber-bullying, use of images or personal information)
- Where the material I research on the internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with permission.
- I will take care to check that information I find on the internet is accurate and understand that some work found on the Internet can be untruthful or misleading.

- I will immediately report any damage or faults involving IT equipment; however this may have happened.
- I will not use any USB storage devices on school's ICT systems.

Pupil Name: _____

Signed: _____

Year: _____

Date: _____

Appendix C

ICT Acceptable Use Agreement - Staff

This agreement applies to the use of all ICT resources inside and/or outside the Trust premises. Staff members are expected to follow all these ICT procedures when using the Trust ICT resources. Failure to follow this agreement may result in disciplinary proceedings. Please note that this agreement takes effect from the moment it is signed and that this may be before your contract start date.

- Prior to being issued with any ICT resource, staff must sign the appropriate procedure form and agree to all outlined procedures.
- Staff members issued with any ICT resources are responsible for its use and care at all times.
- I must not install any software or change the system settings in any way.
- It is expected that I will protect any ICT resource from theft or damage.
- I must not browse, download, or send material that could be considered offensive/illegal.
- Any accidental access to inappropriate materials must be reported to the Lead Person.
- I will ensure that personal data (such as data held on the schools MIS) is kept secure and is used appropriately, whether in school, out of school or remotely.
- I will not use any USB storage devices.
- Personal data can only be taken out of school if authorised by the Lead Person.
- I will not use any personal device to record audio or video of other students or adults without their explicit consent.
- I will not communicate with pupils through social media sites.
- I will ensure all my privacy settings on social media sites are set appropriately.
- I will ensure that any use of social media sites will not bring my role into disrepute.
- I will not use my personal devices or e-mail address to communicate with pupils or parents.
- I will not give out my personal details to pupils or parents.
- Upon the Trust request I will provide immediate access to any ICT equipment that has been assigned to me.
- If any ICT resource is lost, damaged or stolen I will notify the Lead Person
- Failure to return the Trust ICT resource will be considered a breach of this agreement and as such the Trust will take any necessary action to recover the cost of its property.

Name _____

Signature _____

Job Title _____

Date _____

Appendix D

Data Breach Form

This template is to be used by schools to record a data breach. Please do not attempt to notify those who have been affected by the data breach until guidance has been sought from the BWCAT Head of Governance.
Please do not complete the grey sections.

This should be completed immediately after a data breach and emailed within four hours of identifying the breach to the Head of Governance to j.johnson@bwcat.org

The Head of Governance will notify the Information Commissioner's Office (ICO) of any data breach within 72 hours after the breach has been identified, if required.

Contact details	
Name of person who raised the issue	
Contact email address of person who raised the issue	
Contact telephone number of person who raised the issue	
Job title	
Today's date	

Incident information	
Type of data breach	
Date and time of data breach	
Date and time breach was noticed (if above is not identifiable yet)	
Action taken when breach was identified	
Identification code of devices involved (if known)	
Description and location of devices	
Description of what caused the breach e.g. human error	
If breach was due to human error, please name the member of staff	
Details of any personal data that was compromised	

Approximate number of data subjects affected	
Identity of user and website or service being accessed (if applicable)	
What is the likely impact of the breach?	
Have persons affected been informed of the breach and when were they informed? Do NOT do this if you haven't. Seek guidance from DPO first.	

For Head of Governance completion	
Have persons affected been informed on how the breach will be rectified?	
Have any external bodies been informed of the breach, e.g. the ICO? State reasons	
Steps taken to prevent further data loss, including changes to existing procedure and refresher training given	
Conclusion	

By signing this form, you agree that the information within this form has been checked and is correct upon date of completion. All information in this form will be stored for school and trust records so that the school and trust can use the information to ensure their security systems are kept safe to minimise risks of a data breach. This will also be used to assess risks and training needs.

Name of person completing this form	
Signed	
Date	

By signing this form, the Head of Governance agrees that the information within this form has been checked and is correct upon date of completion. All information in this form will be stored for school and trust records so that the school and trust can use the information to ensure their security systems are kept safe to minimise risks of a data breach.

Name of BWCAT Head of Governance	
Signed	
Date form completed	

The 16 schools in our Trust:

St. Mary's Menston, a Catholic Voluntary Academy

St. Joseph's Catholic Primary School Otley, a Voluntary Academy

Ss Peter and Paul Catholic Primary School, a Voluntary Academy

Sacred Heart Catholic Primary School Ilkley, a Voluntary Academy

St Mary's Horsforth Catholic Voluntary Academy

St. Joseph's Catholic Primary School Pudsey, a Voluntary Academy

St Joseph's Catholic Primary School Harrogate, a Voluntary Academy

St Mary's Catholic Primary School Knaresborough, a Voluntary Academy

St. Stephen's Catholic Primary School and Nursery, a Voluntary Academy

Holy Name Catholic Voluntary Academy

St Roberts Catholic Primary School, a Voluntary Academy

St John Fisher Catholic High School Harrogate, a Voluntary Academy

St Joseph's Catholic Primary School Tadcaster, a Voluntary Academy

Barkston Ash Catholic Primary School, a Voluntary Academy

St Joseph's Catholic Primary School Barnoldswick, a Voluntary Academy

St Wilfrid's Catholic Primary School, a Voluntary Academy

The Bishop Wheeler Catholic Academy Trust

The Bishop Wheeler Catholic Academy Trust is a charity and a company limited by Guarantee, registered in England and Wales.

Company Number: 8399801

Registered Office: Bradford Road Menston, LS29 6AE

Website: www.bishopwheelercatholicacademytrust.org

Tel: 01943 883000

Email: j.johnson@bwcat.org

Chair of the Trust Board: Mrs Helen Mills