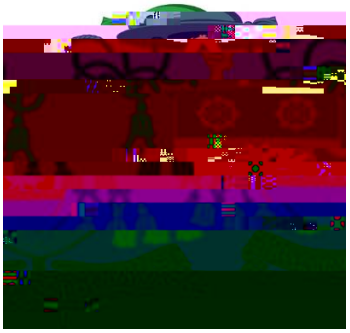
The Bishop Wheeler Catholic Academy Trust



Our Mission

	3.0
	24/10/23
	Mr D. Beardsley

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

refers to The Bishop Wheeler Catholic Academy Trust.

covers all the schools within The Bishop Wheeler Catholic Academy Trust and The Bishop Wheeler Catholic Academy Trust Office.

refer to children and young people under the age of 18 years.

means the Trust Board and the CEO (Chief Executive Officer).

refers to a third-party business that provides ICT services.

refers to:
COO (Chief Operating Officer) for the Trust Office.
Executive Headteacher/Headteacher of the academy.

refers to any person who holds parental responsibility for the child, to include relatives and family friends that may be present at school led events.

Refers to Information and Communication Technologies.

Refers to Multi Factor Authentication, which is used as an additional security layer to protect Trust data.

includes, but not limited to: laptops, desktop computers, mobile phones, iPods, iPads, cameras, printers, televisions, DVD players and any other device which is capable of storing, displaying, receiving or transmitting data.

refers to an ICT system not hosted within the Trusts private premises.

means a digital system used to manipulate, store, retrieve or display-data and the people who use them.

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 wit

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.

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 for KS1 and KS2 pupils, for KS3, KS4 and KS5 pupils and for staff.

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

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 a00 0 1 2588W5.4(m)9(en)]TJETQ0.000008871 0 595.32

5. The Lead Person to

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

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.

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.

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

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

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.

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 _____

Pupil Name: _____

Signed: _____

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

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
