Bradford Diocesan Academies Trust

ACCEPTABLE USE OF IT POLICY

Issued: May 2016
Reviewed: December 2021
Updated: September 2023
Next Review Due: January 2024

Introduction

The Trust's ICT Acceptable Use policy is divided into the following three sections.

1) General policy and code of practice
2) Internet policy and code of practice
3) E-mail policy and code of practice

This policy should also be read in accordance with the Trust's Social Media policy.

Privacy

In particular, please note the provisions set out in this ICT policy about privacy and how the Trust may monitor data, information and material in relation to or used, sent or received by you.

Section One - General policy and code of practice introduction

In March 2021 the BDAT Board approved a contract with Our Learning Cloud (OLC) to procure a cross Trust digital infrastructure upgrade and ongoing managed service for ICT services for the central office and all academies within the Trust. All schools were migrated onto this platform by May 2022.

The government have mandated that all schools and MATs comply with cyber security regulations following an increasing number of cyber-attacks. A heavy investment has been made across the Trust in bringing the central office and all academies to an equitable, secure, and good minimum specification of ICT. Trust wide procurement has ensured that all academies' ICT provision is fit for purpose, resilient, and compliant. From May 2022, the central office and all academies moved from onsite or partial cloud networks to a single domain, cyber essential compliant BDAT cloud. This is hosted and managed by OLC supported by Microsoft, and the tenancy is be owned by BDAT.

The central office and all academies are supported by an OLC led managed service consisting of some onsite support but also access to a large support desk. Staff are able to log tickets, with most tickets being resolved remotely due to the cloud based system.

The Trust intends that you will use and benefit from its well developed and advanced ICT systems. The policy set out below sets out the rules that you must comply with to ensure that the system works effectively for everyone.

In the following guidance, Trust and Academies have equal meaning and are interchangeable.

PRIVACY

The Trust will try to respect your privacy but in order to protect students' safety and well-being and to protect the Trust from any third party claims or legal action against it, the Trust may view any data, information or material on the Trust's ICT system (whether contained in an e-mail, on the network, notebooks or laptops) and in certain circumstances, disclose that data, information or material to third parties, such as the police or social services. You consent to the Trust viewing, using and disclosing data, information or material in relation to, used, sent or received by you.

The Trust's disclaimer which automatically appears at the end of each of your e-mails notifies the recipient that any e-mail correspondence between you may be monitored. You must not remove this disclaimer. You should bring to the attention of any person who wishes or intends to send you an e-mail that the Trust may monitor the content of their e-mail.

Code of practice

Trust's philosophy	In using ICT, you will follow the Trust's ethos and consider the work and feelings of others. You must not use the system in a way that might cause annoyance or loss of service to other users.
Times of access	The network is available during term time. Out of term time the network may be subject to maintenance downtime and so may not be available for brief periods.
User ID and password and logging on	You will be given your own user ID and password. You must keep these secret and not tell or show anyone what they are. Your password must be at least eight characters long and a mixture of capitals, lower case letters, numbers and symbols. If you forget or accidentally disclose your password to anyone else, you must report it immediately to a member of the ICT support staff by either logging a ticket or informing an onsite technician. You must not use another person's account or allow another person to use your account. The facilities are allocated to you on a personal basis and you are responsible for the use of the machine when you are logged on. Use of the Trust's facilities by a third party using your username or password will be attributable to you, and you will be held accountable for the misuse. You must not log onto more than one computer at the same time.
Printing at work	The Trust may wish to check that expensive resources are being used efficiently and so a member of ICT staff may suggest other strategies to you in order to save on resources.
Printing at home	If staff wish to print at home using a personal printer, they must log a ticket with OLC. An OLC technician may need to remote onto your device to install the necessary printer drivers. There are potential security risks associated with this, but you must ensure that you store and dispose of confidential documents that you have printed at home in the correct way. Confidential documents that are printed must be kept in a secure location, such as a locked cabinet or drawer, until you are able to return to work and dispose of them in a secure shred bin. You must not discard confidential documents in your ordinary household waste bin. If you need to dispose of them at home then you must use a shredder.
Logging off	You must log off from the computer you are using at the end of each of your sessions and wait for the standard login screen to reappear before leaving. This signals to the system that you are no longer using the service, it ensures security and frees up resources for others to use.
Access to information not normally available	You must not use the system or the internet in order to find or use facilities or flaws in the system that might give access to information or areas of the network not normally available. You must not attempt to install software to explore or harm the system. Use of hacking tools e.g. 'loggers', 'sniffers' or 'evidence elimination software' is expressly forbidden, particularly given the government cyber compliance regulations in place.

Connections to the system	You must not connect any hardware which may be detrimental to the Trust network.
Connections to the computer	You should use the keyboard, mouse and any headphones provided. You must never attempt to use any of the connectors on the back of any desktop computer. You are not permitted to connect anything else to the computer without first getting the permission of a member of the ICT staff, including USB memory sticks as memory sticks can contain vicious malware.
Virus	If you suspect that your computer has a virus, you must report it to a member of the ICT staff immediately.
Installation of software, files or media	You must not install or attempt to install software of any kind to network drives or local hard drives of networked desktop computers. You must not alter or re-configure software on any part of the Trust's system.
File space	You must manage your own file space by deleting old data rigorously and by deleting emails that you no longer require. If you believe that you have a real need for additional space, please discuss this with a member of the ICT support staff.
Reporting faults and malfunctions	You must report any faults or malfunctions by logging a ticket to the helpdesk including full details and all error messages as soon as possible.
Food and drink	You must not eat or drink nor bring food or drink, including sweets and chewing gum, into the ICT rooms. You must maintain a clean and quiet working environment at all times.
Copying and plagiarising	You must not plagiarise or copy any material which does not belong to you.
Copies of important work	Data is regularly backed up via the cloud system, removing the need for staff to keep backup copies on CDs or saving work onto a memory stick. Staff are permitted to keep paper copies of important documents if they wish but must store and dispose of them as per the 'Printing at home' section.
Security	Laptops and mobile storage devices used for storing sensitive or person al data must be protected by password, PIN, biometrics or encryption to prevent unauthorised access and to be GDPR compliant. Multi Factor Authentication (MFA) will be used by all Trust staff under OLC's system. The use of MFA further strengthens the Trust's cyber security processes.
Bring Your Own Device (BYOD) Wi-Fi / Guest Wi-Fi	Staff, volunteers, and visitors using either the BYOD or Guest Wi-Fi systems at a BDAT site through a Trust device or a personal device must adhere to this code of practice and policy at all times.
Smartwatches	Staff, volunteers, and visitors who wear a smartwatch in school must ensure that this is on silent mode and is not used during the working day other than to read the time.

Section Two - Internet policy and code of practice Introduction

The Trust is able to provide access to the internet from desktop PCs via the computer network and through a variety of electronic devices connected wirelessly to the network. Whenever accessing the internet using a Trust device or your own personal device, you must observe the code of practice below. This code of practice and policy is designed to reduce and control the risk of offences being committed, liabilities being incurred, staff, volunteers or other students being offended and the Trust's facilities and information being damaged.

Consequently, any breach of this policy and the code of practice will be treated extremely seriously and it may result in disciplinary or legal action. The Trust may take steps, including legal action where appropriate, to recover from an individual any expense or liabilities it incurs as a result of the breach of this policy and code of practice by you.

Why is internet access available?

The internet is a large and very useful source of information. Numerous websites and services, both official and unofficial, provide information or links to information which would be beneficial for educational purposes.

Why is a code of practice necessary?

There are four main issues:

- Although the internet is often described as 'free', in fact there is a significant cost to the Trust for using it. This cost includes subscription costs (which may depend on how much a service is used) and the computer hardware and software needed to support internet access.
- Although there is much useful information on the internet, there is a great deal more material which is misleading or irrelevant. Using the internet effectively and safely requires training and self-discipline. Training is available on request from the OLC training team. Relevant modules can also be assigned to colleagues via the Every system.
- Unfortunately, the internet carries a great deal of unsuitable and offensive material. It is important for legal reasons, reasons of principle, and to protect the Trust's staff, volunteers and the students, that access to this unregulated resource is properly managed by the Trust. Accessing certain websites and services and viewing, copying or changing certain material, could amount to a criminal offence and give rise to legal liabilities.
- There is a danger of importing viruses on to the Trust's network, or passing viruses to a third party, via material downloaded from or received via the internet, or bought into the Trust on disk or other storage media.

Bradford Diocesan Academies Trust

Code of practice

Use of the internet	The Internet should not normally be used for private or leisure purposes; it is provided primarily for education or business use. You may use the internet for other purposes provided that: • Such use is occasional and reasonable; • Such use does not interfere in any way with your duties; and • You follow the code of practice at all times.
Inappropriate material	You must not use the internet to access any newsgroups, links, list-servers, web pages or other areas of cyberspace that could be considered to be offensive because of pornographic, indecent, racist, violent, illegal, illicit, or other inappropriate content. "Inappropriate" in this context includes material which is unsuitable for viewing by Trust children. **You are responsible for rejecting and reporting any links to such material which may appear inadvertently during research.** If you encounter any material which could be regarded as offensive you must leave that website or service immediately and not make any copy of that material. If you encounter any difficulty in leaving a website or service, you must inform the ICT support staff immediately.
Misuse, abuse and access restrictions	You must not misuse any inappropriate websites or attempt to bypass any access controls or restrictions on any website or service.
Monitoring	The internet access system used by the Trust maintains a record which identifies who uses the facilities and the use that you make of them. The information collected includes which website and services you visit, how long you remain there and which material you view. This information will be analysed and retained, and where there is evidence that there may have been misuse or abuse of access it may be used in disciplinary and legal proceedings.
Giving out information	You must not give any information concerning the Trust, its students or parents/carers or any member of staff when accessing any website or service. This prohibition covers the giving of names of any of these people, the only exception being the use of the Trust's name and your name when accessing a service which you have been directed to use by the Trust.
Personal safety	You should take care with whom you correspond. You should not disclose where you are nor arrange meetings with strangers you have got in contact with over the internet.
Hardware and software	You must not make any changes to any of the Trust's hardware or software. This prohibition also covers changes to any of the browser settings. The settings put in place by the Trust are an important part of its security arrangements and making any changes, however innocuous they might seem, could allow hackers and computer viruses to access or damage its systems.
Copyright	You should assume that all material on the internet is protected by copyright and must be treated appropriately and in accordance with the owner's rights. You must not copy, download or plagiarise material on the internet unless the owner of the website expressly permits you to do so.

Bradford Diocesan Academies Trust

Section Three - E-mail policy and code of practice

Introduction

The Trust's computer system enables members of the Trust to communicate by e-mail with any individual or organisation with e-mail facilities throughout the world.

For the reason outlined above, it is essential that a written policy and code of practice exists, which sets out the rules and principles for use of e-mail by all.

A copy of this policy and code of practice is included in the staff and student handbooks and on the Trust's intranet. Any breach of this policy and code of practice will be treated seriously and it may result in disciplinary or legal action or expulsion. The Trust may take steps, including legal action where appropriate, to recover from an individual any expense or liabilities it incurs as a result of the breach of this policy and code of practice by you.

Code of practice

Purpose	You should only use the Trust's e-mail system Trust for Trust related emails.
Trust's disclaimer	The Trust's e-mail disclaimer is automatically attached to all outgoing e-mails and you must not cancel or disapply it.
Monitoring	Copies of all incoming and outgoing e-mails, together with details of their duration and destinations are stored centrally (in electronic form). **The frequency and content of incoming and outgoing external e-mails are checked from time to time** to determine whether the e-mail system is being used in accordance with this policy and code of practice. The CEO, Headteacher/Principal, senior staff and technical staff are entitled to have read-only access to your e-mails.
Security	As with anything else sent over the internet, e-mail is not completely secure. There is no proof of receipt, e-mails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents. As with other methods of written communication, you have to make a judgment about the potential damage if the communication is lost or intercepted. Never send bank account information, including passwords, by e-mail.
Program files and non-business documents	You must not introduce program files or non-business documents from outside onto the Trust's network. This might happen by opening an e-mail attachment or by downloading a file from a web site. Although virus detection software is installed, it can never be guaranteed 100% successful, so introducing non-essential software is an unacceptable risk for the Trust. If you have any reason for suspecting that a virus may have entered the Trust's system, you must contact the ICT support staff immediately.

Quality	E-mails constitute records of the Trust and are subject to the same rules, care and checks as other written communications sent by the Trust, so, for example: • You should always consider whether it is appropriate for material to be sent to third parties; • They may have to be disclosed in legal proceedings; • They may have to be disclosed to a person if they makes a request to see information held about them under data protection law; • They may require the same level of authorisation before being sent; • Printed copies of e-mails need to be retained in the same way as other correspondence; • They are confidential to the sender and recipient, unless you have been given permission to read them; • Transmitting the works of others, without their permission, may infringe copyright; • Sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libellous, malicious, threatening or contravening discrimination legislation or detrimental to the Trust may be dealt with under the Disciplinary Policy and Procedure and may also be a legal offence.
Inappropriate e-mails or attachments	You must not use e-mail to access or send offensive material, chain messages or list-servers or for the purposes of bullying or plagiarising work. You must not send personal or inappropriate information by e-mail about yourself, other members of staff, students or other members of the Trust community, or any other individual or organisation. If you receive any inappropriate e-mails or attachments, you must report them to the relevant member of ICT staff.
Viruses	If you suspect that an e-mail has a virus attached to it, you must inform the relevant member of ICT staff immediately.
Spam	You must not send spam (sending the same message to multiple e-mail addresses) without the permission of senior staff.
Storage	Old e-mails will be deleted from the Trust's server after 6 months. You are advised to regularly delete material you no longer require and to archive material that you wish to keep.
Message size	Staff and volunteers are limited to sending messages with attachments which are up to 2MB in size. If you wish to distribute files within the Trust, you can do so by using shared areas e.g. via a shared Launchpad.
Confidential Emails	You must ensure that confidential emails are suitably protected at all times by using encryption or passwords. If working at home or remotely, you should be aware of the potential for an unauthorised third party to be privy to the content of the email. Confidential emails should be deleted when no longer required.

E-MAIL POLICY – advice to staff and volunteers

Staff should be guided by the following good practice:

1. Wherever possible and where time allows, staff and volunteers should check their e-mails on a daily basis and respond, as appropriate, within a reasonable period if the e-mail is directly addressed to them.
2. Staff and volunteers should avoid Spam. Staff should avoid using the e-mail system as a message board and thus avoid sending trivial global messages. Whilst accepting the convenience of the Staff-Academic Distribution list staff should try to restrict its use to important or urgent matters.
3. Staff and volunteers should send e-mails to the minimum number of recipients.
4. Staff and volunteers are advised to create their own Distribution lists, as convenient and appropriate.
5. Staff and volunteers should always include a subject line.
6. Staff and volunteers are advised to keep old e-mails for the minimum time necessary.

Further guidelines:

- Remember - E-mails remain a written record and can be forwarded to others or printed for formal use.
- As a rule of thumb, staff and volunteers should be well advised to only write what they would say face to face, and should avoid the temptation to respond to an incident or message by e-mail in an uncharacteristic and potentially aggressive fashion. Remember "Tone" can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression.
- Remember that sending an email from your Trust account is similar to sending a letter on Trust letterhead, so don't say anything that might bring discredit or embarrassment to yourself or the Trust.
- Linked with this, and given the popularity and simplicity for recording both visual and audio material, staff and volunteers are advised to remember the possibility of being recorded in all that they say or do.