Bishop Chadwick
Catholic Education Trust

Bishop Chadwick Catholic Education Trust

Acceptable Use of IT Systems Policy
September 2020

Agreed by Directors: 20 October 2020
Review Date: Autumn 2021

Table of Contents

1. Revision History

The below table provides the revision history for this document. Each revision has an associated date, issue number, and description of the changes and/or content. The document revisions appear in descending order, with the most-recent iteration appearing first in the table.

Date	Version	Description	Author
23/09/2020	0.a	Initial Draft	Sarah Burns

2. Document Approval

Document Name	Acceptable Use of IT Systems Policy	
Publication Date		
Prepared by	Sarah Burns (DPO)	
Approval (Name & Organization)	Name	Sign

3. Purpose

The purpose of this policy is to ensure that the Bishop Chadwick Catholic Education Trust (the Trust) IT systems are used in a way that minimises the risks of any information security or data protection breaches.

The overall objective of this policy is to ensure that employees, associates, contractors and agency staff adhere to the Data Protection and Information Security obligations placed upon them by the legislation which currently includes (and is not limited to) the General Data Protection Regulation, the Data Protection Act (2018) and the Computer Misuse Act (1990) and to support adherence to all other relevant Trust Information Security Polices.

The Trust is committed to ensuring that it complies with all legal and regulatory requirements when conducting its business activities.

4. Scope

This 'Acceptable Use of IT Systems' Policy covers the security and use of all Trust IT systems including the use of email, internet, voice and mobile IT equipment.

Additional process, standards or procedure documentation may be implemented at a school level to support the minimum requirements outlined within this policy, it should be interpreted such that it has the widest application, so as to include new and developing technologies and uses, which may not be explicitly referred to in this policy.

This policy applies to all employees (permanent and temporary), associates, contractors and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form relating to the Trust's business activities, and to all information handled by the Trust and third parties with whom it deals with. It also covers all IT and information communication facilities operated by or on behalf of the Trust.

The Trust has no appetite for any regulatory breaches and will never knowingly / intentionally breach any applicable law or regulation relevant to the conduct of its business activities. The Trust has a very low risk appetite to breaches of this policy and its associated polices, standards and controls and procedures.

5. Policy Statement

Data Protection Legislation

At the time this policy was written, it aims to satisfy data protection legislation in the United Kingdom which are; -

- The General Data Protection Regulation (GDPR)
- Privacy and Electronic Communications Regulations (PECR)
- The UK Data Protection Act 2018

Where there are changes made to the above legislation, this policy and related policies will be reviewed to assess if any updates are required.

It is the Trust policy to:

- promote and facilitate the positive and extensive use of Information Technology in the interests of supporting the delivery of learning, teaching and innovation to the highest possible standards. This also requires appropriate and legal use of the technologies and facilities made available to students and employees;

- have appropriate technical and organisational measures to ensure continued compliance with the data protection act and GDPR which includes ensuring individuals (employees, contractors and agents) are aware of their obligations and issue rules and instructions (via relevant policies and procedures) on what individuals are (and are not) permitted to do;

- ensure information is only accessed by those who have appropriate authority to do so;

- ensure authorised users have access to information and associated assets only as and when required within a need to know basis;

- ensure all data and confidential information that the Trust manages is suitably secure to protect against consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information;

- meet all data protection and information security requirements under the relevant regulations, legislation, organisational policies / procedures and contractual obligations;

- ensure the security and integrity of all its data, services and processes by ongoing reviews and oversight of all new and existing data privacy risks, to ensure appropriate controls are operating effectively or implemented and documented when any new risks are identified;

- provide a secure working environment for all individuals supporting the Trust;

- require all individuals to ensure that the security, confidentiality and integrity of the data they are handling is suitably robust;

- promote this policy and raise awareness of data privacy;

- provide appropriate data privacy training for individuals and where relevant, connected third parties.

Important

It is of critical importance that you do not communicate with pupils or ex-pupils under the age of 18 using social media without the express permission of the CEO of the Trust. Any social media communication must be done through official Trust/school social media accounts that Trust senior leaders and the school SLT are aware of.

Failure to comply with this may result in disciplinary action which could lead to dismissal.

6. System Access Control – Individual Responsibilities

Access to the Trust IT systems is controlled by implementing user IDs, passwords and/or tokens. All user IDs and passwords are to be uniquely assigned by authorised personnel only to named individuals and consequently, **individuals are accountable for all actions on the Trust's IT systems.**

Individuals must not:

- Allow anyone else to use their user ID/token and password on any Trust IT system;
- Leave their user accounts logged in at an unattended and unlocked computer;
- Use someone else's user ID and password to access the Trust's IT systems;
- Leave their password unprotected (for example writing it down);
- Perform any unauthorised changes to the Trust IT systems or information;
- Attempt to access data that they are not authorised to use or access;
- Exceed the limits of their authorisation or specific business need to interrogate the system or data;
- Connect any non-Trust authorised device to IT systems or network;
- Store Trust data on any non-authorised equipment;
- Give or transfer Trust data or software to their own personal devices or any person or organisation outside of the Trust without the authority of the Trust;
- Line managers must ensure that individuals are given clear direction on the extent and limits of their authority regarding access to the Trust IT systems and data.

7. Internet and Email Conditions of Use

Use of the Trust's internet and email is intended for work related use only. Personal use of the Internet is permitted for example in lunch periods where such use does not affect the individual's work performance, is not detrimental to the Trust in any way, not in breach of any terms and conditions of employment and does not place the individual or Trust in breach of statutory or other legal obligations. Personal use of the email is not permitted.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse;
- Use profanity, obscenities, or derogatory remarks in communications;

- Access, download, send or receive any data (including images), which the Trust considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material;
- Use the internet or email to make personal gains or conduct a personal business;
- Use the internet or email to gamble;
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam;
- Place any information on the Internet that relates to the Trust, alter any information about it, or express any opinion about the Trust, unless they are specifically authorised to do this
- Send unprotected personal or confidential information externally;
- Forward any related Trust email to personal (non-Trust) email accounts (for example a personal Hotmail account)
- Make official commercial commitments through the internet or email on behalf of the unless authorised to do so;
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval;
- In any way infringe any copyright, database rights, trademarks or other intellectual property;
- Download and install any software from the internet without prior approval of the IT Department.

8. Clear Desk and Clear Screen Standards & Controls

In order to reduce the risk of unauthorised access to or loss of information, the Trust enforces the following clear desk and clear screen standards and controls:

- Personal or confidential work related information must be protected using security features provided for example, the use of company approved secure printers;
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when left unattended;
- Care must be taken to not leave confidential paper material on printers or photocopiers;
- All business-related printed material that is no longer needed must be disposed of using confidential waste bins/bags or shredders;
- Desks should be left clear of all confidential paper documents at the end of each working day;
- Confidential papers should be secured in lockable pedestals and cupboards (where provided);
- Confidential papers should not be left in meeting rooms once a meeting has finished;
- White boards and flip charts should be cleared of all information following a meeting.

9. Remote working (working off-site)

It is accepted that laptops and mobile devices can be taken off-site if required however the following controls **must** be applied:

- Equipment and media taken off-site must not be left unattended in public places and not left in plain sight within a car;

- Laptops must be carried as hand luggage when travelling on any public service journey;
- Care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption;
- Screen lock electronic devices when not in use;
- Use caution when working on any company or customers data whilst outside the office (e.g. during a train journey when other passengers may be able to view the information you are working on);
- Individuals should take care if discussing any commercial or customer matters outside of the office where other members of the public are able to overhear conversations.

Theft or Loss or damage of Bishop Chadwick Catholic Education Trust equipment

All individuals are obligated to take extra care when using Trust IT devices outside of the workplace. Individual safety is of utmost importance to the Trust so you should not attempt to protect any company equipment if there is a potential risk to your health or wellbeing. If any device is lost or stolen individuals must:

- Report the loss or theft to their Line Manager as soon as they become aware;
- Line Managers/ Headteachers are responsible for notifying the loss or theft to the DPO or COO;
- Consideration should be given regarding onward reporting to the Police;
- Any damaged equipment must be returned to the IT department, individuals must not attempt to dispose of broken equipment themselves.

10. Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data and where authorisation is granted by the Headteacher. In such situations a Data Protection Impact Assessment (DPIA) should be completed to assess and mitigate any potential risks. Only the Trust authorised mobile storage devices with encryption enabled must be used, when transferring personal, sensitive or confidential data.

11. Software & Viruses

Software

Individuals must use only software that is authorised by the Trust and on the Trust's computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on the Trust's computers must be approved and installed by the relevant Trust IT department.

Viruses

The IT department has implemented centralised, automated virus detection and virus software updates within the Trust. All PC's have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection.

12. Telephony and Photography

The Bishop Chadwick Catholic Education Trust telephones are intended for work related use, unless approval from the Headteacher in granted.

Individuals must not:

- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for business use.

PHOTOGRAPHY

All photography taken within the school for educational purposes should be formally approved by the Headteacher. Whilst the Trust understands that most people will have camera phones they must:

- Make sure no personal or confidential data appears in the photo (consider computer screens that may be on show or paper documents on desks);
- Think carefully before posting any workplace photos on social media (they often reveal more about the Trust and security than individuals may think);
- Never take any photographs of any computer screens, especially any photographs of personal or confidential data as this will be considered a breach of security leading to a possible disciplinary offence.

13. Termination of Contract

All the Trust's IT equipment and data, for example laptops and mobile devices including telephones, smartphones and CDs/DVDs, must be returned to the Trust immediately upon termination of contract.

All Trust data or intellectual property developed or gained during the period of employment remains the property of the Trust and must not be retained beyond termination or reused for any other purpose.

14. Monitoring & Filtering

All data that is created and stored on the Trust computers is the property of the Trust and whilst complying with Data Regulation, there is no official provision for individual data privacy, however wherever possible the Trust will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. The Trust has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018, the General Data Protection Regulation, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

It is the responsibility of all individuals to report suspected breaches of security policies without delay to the Headteacher, the IT department or a Trust Director/DPO in line with the GDPR Data Breach Process.

All breaches of information security and data protection policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with the Bishop Chadwick Catholic Education Trust disciplinary procedures.

15. Security Risks

While acceptable usage of IT systems can prevent many security risks, individual actions are also important when applying information security or data protection requirements. Its therefore important to ensure to;

- use extreme caution when opening email attachments from unknown senders or unexpected attachments from any sender;
- be on guard against social engineering, such as attempts by outsiders to persuade you to disclose confidential information, including employee, pupil or school confidential information;
- be wary of fake websites and phishing emails;
- don't click on links in emails or social media;
- don't disclose passwords and other confidential information unless you have confirmed identity and need to know principle;
- use social media, including personal blogs, in a professional and responsible way, without violating policies or disclosing confidential information;
- take particular care of IT assets when you are away from home or out of the office;
- follow clear desk requirements ensuring paper based confidential information is secured where unauthorised people cannot see it and shredded when no longer required;

If you notice any signs of unusual or suspicious events which could lead to a potential or actual security breach it should be reported immediately in line with the GDPR Data Breach Process.

Examples of such events are as follows:

- Unexpected system or application crashes;
- Abnormal slow running of a laptop;
- Signs of physical tampering to a laptop device.

16. Definitions

Trust means all schools within the Bishop Chadwick Catholic Education Trust who process Personal Data.

COO means the Chief Operating Officer

DPO means the Data Protection Officer, the individual within the Bishop Chadwick Catholic Education Trust who has oversight for Data Privacy compliance.

GDPR means the General Data Protection Regulation (EU) 2016/679 which is a regulation in EU law on data protection and privacy for all individuals within the European Union.

Individuals means any employee, contractor, agent who any such person employed on behalf of the Bishop Chadwick Catholic Education Trust

Personal Data means data relating to a living individual.

Policy means the GDPR Acceptable Use of IT Systems Policy.

The Bishop Chadwick Catholic Education Trust Systems means any system, device and equipment owned by The Bishop Chadwick Catholic Education Trust.