IT SECURITY POLICY

Approved by Audit Committee 12 May 2020

Contents

1. Introduction

The Blessed Christopher Wharton Catholic Academy Trust takes the safeguarding and handling of data very seriously, this document (and supporting policies) governs the processing of Personal Data, and defines the technical and security measures that must be implemented in order to meet the requirements of the European Union's General Data Protection Regulation (GDPR) and the Data Protection Act 2018, and ensure integrity and availability of the data environment and services

2. Purpose

The purpose of this policy is to protect The Blessed Christopher Wharton Catholic Academy Trust, its stakeholders and staff from all information security threats, whether internal or external, deliberate or accidental. BCWCAT is critically dependent on information and information systems. If important information were disclosed to inappropriate persons, the company could suffer serious losses or go out of business. The good reputation that BCWCAT enjoys is also directly linked with the way that it manages both information and information systems.

Information security is characterised as the preservation of:

- Confidentiality- ensuring that information is accessible only to those authorised to have access.
- Integrity- safeguarding the accuracy and completeness of information and processing methods.
- Availability- ensuring that authorised users have access to information and associated assets when required.
- Regulatory compliance: ensuring that BCWCAT meets its regulatory and legislative requirements.

3. Scope

This policy applies to the following areas listed below:

Involved Persons - BCWCAT Trustees, Academy Councillors, volunteers and all staff must comply with the information security policies found in this and any related information security documents.

BCWCAT Trustees, Academy Councillors, volunteers and all staff, contractors and third-party users should be made aware of this policy, their responsibilities and liabilities, and any information security threats or concerns.

Involved Systems -

- All information owned by the BCWCAT independent of who processes the information.
- Information and information systems in all forms, independent of the medium on which they are held (physical, electronic) or the form which they take (text, graphics, software, databases, multi-media).
- All stages of the information lifecycle: creation, use, storage, disposal.
- The transmission of information independent of means (post, electronic, oral).
- All authorised users of BCWCAT's information and information systems, whether or not they are staff.
- Software: BCWCAT's operating system software and support programs, application software, application enabling software
- Location: permanent or temporary offices, home/mobile working locations, institutes, establishments and laboratories operated by the BCWCAT or wherever information associated with the BCWCAT is located.

4. Roles and Responsibilities

All individuals who use BCWCAT information or information systems have a duty of care to protect the confidentially of information that is entrusted to them. The principal information security responsibilities for all are to:

- Only use information and information systems that you have authorisation to use.
- Follow all relevant instruction, procedures, guideline and codes of practice.
- Report any real or suspect breaches of information security to your line manager
- Not use, or attempt to use, any information or information system for illegal of inappropriate purposes

Three Categories Of Responsibilities - To coordinate a team effort, BCWCAT has established three categories, at least one of which applies to each worker. These categories are Owner, Custodian, and User. These categories define general responsibilities with respect to information security.

i. **Owner Responsibilities** - Information Owners are the department managers, members of the top management team, or their delegates within BCWCAT who bear responsibility for the acquisition, development, and maintenance of production applications that process BCWCAT information.

Production applications are computer programs that regularly provide reports in support of decision-making and other business activities. All production application system information must have a designated Owner.

For each type of information, Owners designate the relevant sensitivity classification, designate the appropriate level of criticality, define which users will be granted access, and approve requests for various ways in which the information will be utilised.

ii. **Custodian Responsibilities** - Custodians are in physical or logical possession of either BCWCAT information or information that has been entrusted to BCWCAT. While Information Technology department staff members clearly are Custodians, local system administrators are also Custodians.

Whenever information is maintained only on a personal computer, the User is also a Custodian.

Each type of production application system information must have one or more designated Custodians.

Custodians are responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and making backups so that critical information will not be lost. Custodians are also required to implement, operate, and maintain the security measures defined by information Owners.

iii. **User Responsibilities** - Users are responsible for familiarizing themselves with and complying with all BCWCAT policies, procedures, and standards dealing with information security.

Questions about the appropriate handling of a specific type of information should be directed to either the Custodian or the Owner of the involved information.

5. Information

6. Classification and Handling

Consistent Information Handling - BCWCAT information, and information that has been entrusted to BCWCAT, must be protected in a manner commensurate with its sensitivity and criticality. Security measures must be employed regardless of the media on which information is stored, the systems that process it, or the methods by which it is moved. Information must be protected in a manner that is consistent with its classification, no matter what its stage in the life cycle from origination to destruction.

Information Classification Designations - BCWCAT has adopted an information classification system that categorizes information into four groupings. All information under BCWCAT control, whether generated internally or externally, falls into one of these categories: Secret, Confidential, Internal Use Only, or Public. All workers must familiarise themselves with the definitions for these categories and the steps that must be taken to protect the information falling into each of these categories. For purposes of this policy, "sensitive information" is information that falls into either the Secret or Confidential categories.

Information Classification Labelling - If information is sensitive, from the time it is created until the time it is destroyed or declassified, it must be labelled with an appropriate information classification designation. Such markings must appear on all manifestations of the information. The vast majority of BCWCAT information falls into the Internal Use Only category. For this reason, it is not necessary to apply a label to Internal Use Only information. Information without a label is therefore by default classified as Internal Use Only. Further instructions about labelling sensitive information can be found in the Information Classification Policy.

7. Information Access Control

6.1 Need to Know

Access to information in the possession of, or under the control of BCWCAT must be provided based on the need to know. Information must be disclosed only to people who have a legitimate business need for the information. To implement the need-to-know concept, BCWCAT has adopted an Access request and Owner approval and Review process.

When an employee's role changes, including termination, transfer, promotion and leave of absence, his or her supervisor must immediately notify the Information Security department.

6.2 User IDs

- **Unique IDs –** To implement the need-to-know process, BCWCAT requires that each worker accessing multi-user information systems have a unique user ID and a private password. These user IDs must be employed to restrict system privileges based on job duties, project responsibilities, and other business activities. Each worker is personally responsible for the usage of his or her user ID and password. We also recommend each worker use MFA where possible for all important accounts and internet facing systems.

- **Anonymous User IDs** - With the exception of electronic bulletin boards, Internet sites, intranet sites, and other systems where all regular users are intended to be anonymous, users are prohibited from logging into any BCWCAT system or network anonymously. Anonymous access might, for example, involve use of "guest" user IDs. When users employ system commands that permit them to change active user IDs to gain certain privileges, they must have initially logged on employing user IDs that clearly indicated their identities.

6.3 Passwords

- **Difficult-to-Guess Passwords** - Users must choose passwords that are difficult to guess. This means that passwords must not be related to one's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address must not be used.

- **Easily Remembered Passwords**- Users can use passwords that are difficult for unauthorised parties to guess if they:

  - string several words together
  - shift a word up, down, left, or right one row on the keyboard
  - bump characters in a word a certain number of letters up or down the alphabet
  - transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word
  - combine punctuation or numbers with a regular word
  - create acronyms from words in a song, poem, or another known sequence
  - deliberately misspell a word

  combine several preferences like hours of sleep desired and favourite colours.

- **Repeated Password Patterns** - Users must not construct passwords with a basic sequence of characters that is then partially changed based on the date or some other predictable factor. Users must not construct passwords that are identical or substantially similar to passwords they have previously employed.

- **Password Constraints** - In line with the most recent guidance issued by the Information Commissioner's Office, the emphasis should be on making Passwords or passphrases difficult or complex to begin with rather than require frequent, enforced changes. Therefore, the password or passphrase must be at least 10 characters long, include upper and lowercase letters and special characters, committed to memory and not written down. The password or passphrase is only to be changed when there is a data breach or whenever a worker suspects that a password/passphrase has become known to another person.

- **Storage** - Passwords or passphrases must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorised persons might discover them. Passwords/passphrases must not be written down in readily decipherable form and left in a place where unauthorised persons might discover them. This includes notebooks in desk drawers and plain text files on computers.

- **Sharing** - If workers need to share computer-resident data, they must use unique log-in credentials with shared access to the required electronic mail, group databases, directory or local area network servers. The shared access should be centrally managed by the system administrator/s.

  When access is shared for electronic mail and other purposes, passwords or passphrases must never be shared with or revealed to others.

System administrators and other technical information systems staff must never ask a worker to reveal their personal password/passphrase. The only time when a password/passphrase should be known by another is when it is issued. These temporary passwords/passphrases must be changed the first time that the authorised user accesses the system. If a user believes that his or her user ID and password/passphrase are being used by someone else, the user must immediately notify the system administrator for the information system.

6.4 Compliance Statement

BCWCAT Trustees, Academy Councillors, volunteers and all staff who wish to use BCWCAT multi-user computer systems must sign a compliance statement prior to being issued a user ID. Where users already have user IDs, such signatures must be obtained prior to receiving annually renewed user IDs.

A signature on this compliance statement indicates the involved user understands and agrees to adhere to BCWCAT policies and procedures related to computers and networks, including the instructions contained in this policy.

6.5 Screenshots

All workers should refrain from taking screenshots that include Personally Identifiable Information (that is, any data that can directly or indirectly identify a data subject e.g. name, email address, IP address, job role etc.) and saving a copy to their desktop or mobile device.

8. Third Party Data Handling

7.1 Release Of Information To Third Parties

Unless it has specifically been designated as public, all BCWCAT internal information must be protected from disclosure to third parties. Third parties may be given access to BCWCAT internal information only when a demonstrable need to know exists, when a BCWCAT non-disclosure agreement has been signed, and when such a disclosure has been expressly authorised by the relevant BCWCAT information Owner.

If sensitive information is lost, is disclosed to unauthorised parties, or is suspected of being lost or disclosed to unauthorised parties, the information Owner and the Information Security department must be notified immediately.

7.2 Third-Party Requests For BCWCAT Information

Unless a member of staff has been authorised by the information Owner to make public disclosures, all requests for information about BCWCAT and its business must be referred to the BCWCAT Central Office. Such requests include questionnaires, surveys, and newspaper interviews.

This policy does not apply to sales and marketing information about BCWCAT products and services, nor does it pertain to customer technical support calls.

If a member of staff is to receive sensitive information from third parties on behalf of BCWCAT, this receipt must be preceded by the third-party signature on a BCWCAT release form confirming that the information was obtained through the appropriate legal procedures.

7.3 External Disclosure Of Security Information

Information about security measures for BCWCAT computer and network systems is confidential and must not be released to people who are not authorised users of the involved systems unless approved by the director of Information Security.

9. Physical Security

8.1 Physical Security

Access to every office, computer machine room, and other BCWCAT work area containing sensitive information must be physically restricted to those people with a need to know.

When left in an unattended room, sensitive information in paper form must be locked away in appropriate containers.

During non-working hours, workers in areas containing sensitive information must lock-up all information.

Unless information is in active use by authorised people, desks must be clear and clean during non-working hours to prevent unauthorised access to information.

Workers must position their computer screens such that unauthorised people cannot look over their shoulder and see the sensitive information displayed.

8.2 Theft Protection

All BCWCAT computer and network equipment must be physically secured with anti-theft devices if located in an open office.

Local area network servers and other multi-user systems must be placed in locked cabinets, locked closets, or locked computer rooms.

Portable computers must be secured with locking cables, in locking cabinets, or secured by other locking systems when in an open office environment but not in active use.

Computer and network gear (excluding phones) may not be removed from BCWCAT offices unless authorised.

10.Network Security

9.1 Internal Network Connections

All BCWCAT stand-alone computers and laptops that store sensitive information, and that are permanently or intermittently connected to internal computer networks must have a password-based access control system approved by the Information Security department.

Users working with all other types of computers must employ the screen saver passwords that are provided with operating systems, so that after a period of no activity the screen will go blank until the correct password is again entered.

Multi-user systems throughout BCWCAT must employ automatic log off systems that automatically terminate a user's session after a defined period of inactivity.

9.2 External Network Connections

All in-bound session connections to BCWCAT computers from external networks must be protected with an approved dynamic password access control system. Dynamic passwords are different each time they are used, and therefore cannot be replayed to gain unauthorised access.

Users with personal computers connected to external networks are prohibited from leaving unattended modems turned-on while data communications software is enabled, unless an authorised dynamic password system has been previously installed.

When using BCWCAT computers, BCWCAT workers must not establish connections with external networks including Internet service providers unless these connections have been approved by the Information Security department.

9.3 Network Changes

With the exception of emergency situations, all changes to BCWCAT computer networks must be documented in a work order request and approved in advance by the Information Technology department.

All emergency changes to BCWCAT networks must be made only by persons who are authorised by the Information Technology department. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorised disclosure of information, and other problems. This process applies to workers and vendor personnel.

9.4 Telecommuting

At management’s discretion, certain qualified workers can do some of their work at home. Permission to telecommute must be granted by each worker’s immediate supervisor.

Internet and Electronic Mail

10.1 Internet Access

Workers are provided with Internet access to perform their job duties, but this access may be terminated at any time at the discretion of a worker’s supervisor. Internet access is monitored to ensure that workers are not visiting sites unrelated to their jobs, and also to ensure that they continue to be in compliance with security policies.

Staff must take special care to ensure that they do not represent BCWCAT on Internet discussion groups and in other public forums, unless they have previously received top management authorization to act in this capacity. Staff must not place BCWCAT material on any publicly accessible computer system such as the Internet unless the posting has been approved by both the information Owner and the Information Technology department.

All information received from the Internet should be considered to be suspect until confirmed by reliable sources.

Staff are prohibited from sending sensitive information, passwords or establishing any electronic commerce arrangements over the Internet unless the Information Security department have evaluated and approved of such arrangements. These and related considerations are discussed in greater detail in the company handbook.

10.2 Electronic Mail (Email)

Every BCWCAT member of staff who uses computers in the course of their regular job duties will be granted an Internet electronic mail address and related privileges.

All BCWCAT business communications sent by electronic mail must be sent and received using this company electronic mail address. All BCWCAT staff must additionally employ a standard electronic mail signature for this email address that includes their full name, job title, business address, and business telephone number.

A personal Internet service provider electronic mail account or any other electronic mail address must not be used for BCWCAT business unless a worker obtains management approval.

When transmitting messages to groups of people outside BCWCAT, workers must always use either the blind carbon copy facility or the distribution list facility. Note that unsolicited electronic mail transmissions to prospects and customers are prohibited.

Emotional outbursts sent through electronic mail and overloading the electronic mail account of someone through a deluge of messages are forbidden.

10.3 Computer Virus Screening

All personal computer users must keep the current versions of approved virus screening software enabled on their computers.

Virus screening software must be used to scan all software and data files coming from either third parties or other BCWCAT groups. This scanning must take place before new data files are opened and before new software is executed.

Staff must not abort antivirus software updates or bypass or turn off the scanning processes that could prevent the transmission of computer viruses.

10.4 Viruses

If staff suspect infection by a computer virus, they must immediately stop using the involved computer and call Datacable. Qualified BCWCAT staff or consultants must complete this task in a manner that minimizes both data destruction and system downtime.

Floppy disks and other magnetic storage media used with the infected computer must not be used with any other computer until the virus has been successfully eradicated and the infected computer must also be immediately isolated from internal networks.

10.5 Clean Backups

All personal computer software must be copied prior to its initial usage, and such copies must be stored in a secure location such as a locked file cabinet. These master copies must not be used for ordinary business activities, but must be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems.

10.6 Software Sources

BCWCAT computers and networks must not run software that comes from sources other than other BCWCAT departments, knowledgeable and trusted user groups, well-known systems security authorities, or established computer, network, or commercial software vendors.

Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from untrusted sources must not be used unless approved by the Information Security department.

10.7 Written Specifications for Information Owners

All software developed by in-house staff, intended to process critical or sensitive BCWCAT information, must have a formal written specification. This specification must include discussion of security risks and controls including access control systems and contingency plans.

The specification must be part of an agreement between the information Owner and the system developer. Macros in spreadsheets and word processing documents are not considered software in this paragraph.

10.8 Security Sign-Off Required

Before being used for production processing, new or substantially changed application systems must have received written approval from the Information Security department for the controls to be employed. This requirement applies to personal computers just as it does to larger systems.

10.9 Formal Change Control

All computer and communications systems used for production processing must employ a documented change control process that is used to ensure that only authorised changes are made.

This change control procedure must be used for all significant changes to production system software, hardware, communications links, and procedures.

10.10 Systems Development Conventions

All production software development and software maintenance activities performed by in-house staff must adhere to Information Technology department policies, standards, procedures, and other systems development conventions. These conventions include the proper testing, training, and documentation.

10.11 Adequate Licenses

BCWCAT management must make appropriate arrangements with software vendors for additional licensed copies, if and when additional copies are needed for business activities.

10.12 Unauthorised Copying

Staff must not copy software provided by BCWCAT to any storage media, transfer such software to another computer, or disclose such software to outside parties without authorisation.

10.13 Backup Responsibility

When using personal computers, BCWCAT Trustees, Academy Councillors, volunteers and all staff must regularly back up the information, or ensure that someone else is doing this for them.

For multi-user computer and communication systems, a system administrator is responsible for making periodic backups.

The Information Technology department must install or provide technical assistance for the installation of backup hardware and software.

All backups containing critical or sensitive information must be stored at an approved off-site location with either physical access controls or encryption. A contingency plan must be prepared for all applications that handle critical production information. It is the responsibility of the information Owner to ensure that this plan is adequately developed, regularly updated, and periodically tested.

11. User Rights and Expectations

11.1 Rights To Material Developed

While performing services for BCWCAT, staff must grant to BCWCAT exclusive rights to patents, copyrights, inventions, or other intellectual property they originate or develop.

All programs and documentation generated by, or provided by workers for the benefit of BCWCAT are the property of BCWCAT. BCWCAT asserts the legal ownership of the contents of all information systems under its control. BCWCAT reserves the right to access and use this information at its discretion.

11.2 Right To Search And Monitor

BCWCAT management reserves the right to monitor, inspect, or search at any time all BCWCAT information systems. This examination may take place with or without the consent, presence, or knowledge the involved staff.

The information systems subject to such examination include, but are not limited to, electronic mail system files, personal computer hard drive files, voice mail files, printer spool files, fax machine output, desk drawers, and storage areas.

Because BCWCAT computers and networks are provided for business purposes only, workers must have no expectation of privacy associated with the information they store in or send through these information systems. BCWCAT management retains the right to remove from its information systems any material it views as offensive or potentially illegal.

11.3 Personal Use

BCWCAT information systems are intended to be used for business purposes only. Incidental personal use is permissible if the use does not consume more than a trivial amount of resources that could otherwise be used for business purposes, does not interfere with worker productivity, and does not pre-empt any business activity.

Use of BCWCAT information systems for chain letters, charitable solicitations, political campaign material, religious work, transmission of objectionable material, or any other non-business use is prohibited.

11.4 Unbecoming Conduct

BCWCAT management reserves the right to revoke the system privileges of any user at any time.

Any conduct that interferes with the normal and proper operation of BCWCAT information systems, which adversely affects the ability of others to use these information systems, or that is harmful or offensive to others is not permitted.

Prohibited Activities

- Unless specifically authorised by the Information Security department, staff must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security.

  Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files.

- Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved by the Information Security department.

  Incidents involving unapproved system hacking, password guessing, file decryption, bootleg software copying, or similar unauthorised attempts to compromise security measures may be unlawful and will be considered serious violations of BCWCAT internal policy.

- Short-cuts bypassing systems security measures, and pranks and practical jokes involving the compromise of systems security measures are absolutely prohibited.

Mandatory Reporting

All suspected policy violations, system intrusions, virus infestations, and other conditions that might jeopardize BCWCAT information or BCWCAT information systems must be immediately reported to admin@bcwcat.co.uk.

Exceptions

The Information Security Manager acknowledges that under rare circumstances, certain staff will need to employ systems that are not compliant with this policy. All such instances must be discussed and authorised by the Information Security manager.

12. Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment.

BCWCAT reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

BCWCAT does not consider conduct in violation of any part of this policy to be within an employee's course and scope of employment, or the direct consequence of the discharge of the employee's duties.

Accordingly, to the extent permitted by law, BCWCAT reserves the right not to defend or pay any damages awarded against employees that result from violation of this policy.

13. Monitoring Compliance & Review

Monitoring compliance

This information security management framework (controls and responsibilities) is subject to internal monitoring, alerting and auditing throughout BCWCAT, and the outcomes from these processes will inform and improve practices as part of the commitment to continual improvement.

Reports on the matters related to this Policy should be provided to the Information Security Manager.

Review of Policy

This Policy will be reviewed at least annually or when significant changes are required.

Revision History			
No	Details	Date	Author
V.1.1	Initial creation	March 2020	
V.1.2			