Bishop Chadwick
Catholic Education Trust

Bishop Chadwick Catholic Education Trust

Information and Cyber Security 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	Information and Cyber Security Policy	
Publication Date		
Prepared by	Sarah Burns (DPO)	
Approval (Name & Organization)	Name	Sign

3. Purpose

Information and Cyber Security is about ensuring that the Bishop Chadwick Catholic Education Trust (the Trust) implements appropriate technical and organisational measures to protect the confidentiality, integrity and availability of all information, in all its forms held by or on behalf of the Trust.

This policy applies to all information, in whatever form relating to the Trust and its associated activities, and to all information handled by the Trust and associated third parties with whom it deals with.

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.

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 associated activities. The Trust has a very low risk appetite to breaches of this policy and its subordinate polices, standards and controls and procedures.

4. Scope

This policy applies to all employees (permanent and temporary), associates, contractors and agents (hereafter referred to as 'individuals') within the Trust and associated schools who process personal data, confidential and sensitive data, wherever it may be stored, processed or transmitted within all areas of the Trust and any third parties working with or on behalf of the Trust.

Information & Cyber Security controls should be proportionate to the risks to ensure the appropriate balance between cost and risk mitigation. It is therefore important for the Trust to set the priorities for Information and Cyber Security as documented within this policy.

These priorities should be focussed on achieving the following objectives for Information Security:

- Protect pupil, parents, employee or any other individual's data from loss or theft or unauthorised changes and respond to breaches effectively.
- Prevent and respond to any organisational interruption caused by Cyber-attack or other malicious or accidental threat event.
- Support wider control objectives through Information & Cyber Security controls (e.g. anti-fraud).
- Protect employee data, the Trusts intellectual property and corporate confidential information.
- Minimise financial loss due to external or internal security breaches.
- Meet regulatory requirements related to Information Security.

5. Policy Statement

The Trusts reliance on information in its widest sense and our school's communities concerns about Cyber Security is why the Trust seeks to minimise, as far as is practicable, the risks to information in all our processes and systems. How information and Cyber risks arise can be found at Appendix 1.

Whilst low level 'issues' are inevitable and part of undertaking our day to day functions, we have no appetite for:

- Any compromise of 'confidential' information that would have a significant detrimental effect upon the Trust; or
- Any large scale or prolonged systemic breaches of 'confidential' information, for example any education records or data relating to employees or third party partners.
- Any unavailability of any business systems beyond their defined recovery time objectives.
- Significant non-compliance with any relevant regulatory legislation or scheme rules, including the Data Protection Act and related legislation. "Significant" in this context means that the non-compliance could attract material financial penalties.

To ensure the effectiveness of our security framework, the Trust relies on adequate line functions, including monitoring and assurance functions, within the Trust and associated schools. The 'Two Lines of Defence' model is a way of explaining the relationship between these functions and as a guide to how responsibilities should be divided:

- **the first line of defence –** functions that own and manage risk, eg Teaching and support staff
- **the second line of defence** - functions that oversee or specialise in risk management and compliance eg School SLT, Headteachers, IT Manager, Data Protection Officer, HR Manager

6. Information Classification

An information classification scheme is one of the critical components of good Information Security and is a fundamental step in protecting against the risks associated with the unauthorised disclosure, use or loss of Trust information. An information classification scheme assists in determining the value and sensitivity of information as well as the protective measures to be applied.

Each associated school within the Trust, its associated schools, as well as the Trust Board, must identify its information assets and should classify them in line with the Classification Scheme (See table below).

Higher value assets (confidential) must be appropriately protected from threats.

Classification Scheme	Definition	Examples
Confidential – RED	Sensitive in nature, carries a risk to Privacy of either the Trust or an individual. If confidentiality is breached could lead to significant financial penalties, reputational damage or emotional distress and physical and material damage to an individual.	Trust sensitive and or personal data relating to Pupils. Particularly confidential data is that relating to pupils health, SEND statement, Pupil premium or free school meals data.
Internal Use Only - AMBER	Everyday information related to the functional activities undertaken within a school/ and or the Trust. This would be the default classification. There could potentially be some minor impact if the information was disclosed outside of the Trust.	Meeting notes, agendas, calendar information (non-confidential), internal memos and emails etc.
Public - GREEN	Public Information with no impact if disclosed.	Publicity communications, public accounts, press release etc.

7. Information & Cyber Risk Management

Information Security and Cyber risks identified must be assessed, documented and action plans developed where remediation or mitigation activity is required.

Information risks should be assessed regularly in the context of the Trust and associated school's activities including but not limited to:

- The introduction of major new technologies.
- Using the services of external providers.
- Permitting access to the Trusts critical systems by external individuals.
- Granting access to systems from external locations.
- Material audit findings or major incidents/ breaches.

8. Information & Cyber Security Education / Awareness

Specific security awareness programmes must be undertaken to promote Information & Cyber Security awareness to all individuals who have access to information.

This training must be included in the induction of new starters (within 4 weeks) and be refreshed regularly (at least every 12 months) and include tailored and appropriate security messages.

9. Data Privacy by Design (and default)

The Trust has implemented appropriate technical and organisational measures for ensuring that, by default, only personal data and information which is necessary for each specific purpose of the processing is processed. Our obligation applies to the amount of personal data collected, the extent of its processing, the period of its storage and its accessibility. Such measures should ensure that personal data is only made accessible to the relevant areas and not issued to an indefinite number of entities or persons.

10. Data Protection Impact Assessments (DPIA)

What is a Data Protection Impact Assessment?

- This is a process to help us identify and reduce the data privacy risks of a project or a change and should be used throughout the development or implementation of a project / change.
- It enables us to analyse how a project or a change may affect the privacy of individuals involved systematically.
- They should also be applied to new projects and also any change item that creates or increases risk to personal data. This to allow greater scope for the project needs to be implemented.
- They should also be used when planning changes to an existing system or BAU process.
- The DPIA should ensure privacy risks are minimised whilst allowing the project / change to meet its objectives.
- Risks can be identified early in the project / change by analysing how data will be used (risks to data subjects such as potential for damage or distress).
- It should also assess the corporate risks to our Company such as the financial and reputational impact of a breach arising from the project (higher risk projects that are likely to be more intrusive are likely to have a higher impact on privacy.

Our DPIA processes should not need to be overly complex or time consuming, but there is an expectation of a certain level of rigour in proportion to the privacy risks arising from the process or project under review.

10. Control Framework

A comprehensive, risk driven control framework for Information and Cyber Security has been established and implemented in line with business risk appetite and achievement of business goals.

The framework incorporates the minimum requirements set out in Appendix 2 of this policy.

12. Third Party Management

Third party access to Company information must be restricted to authorised persons only. Third parties and service providers must be:

- Uniquely identified, typically by business owners.
- Be subjected to a due diligence/ data assurance check to ensure adequate controls are in place to protect information appropriately.
- Categorised from an Information Security risk perspective.
- Governed by contracts.
- Monitored in terms of security performance.

13. Incident Management

All employees, and any third parties working for or on behalf of the Trust must report any security breach or incident affecting the Trust to their line manager, Headteacher, IT Manager or DPO immediately they become aware of it.

The Trust will report the necessary details of data and information security breaches, to any relevant regulator or regulated partner in accordance with applicable legislation and regulations.

Definitions

Availability means information being accessible and usable upon demand.

Trust means the Bishop Chadwick Catholic Education Trust and associated schools who process confidential information, personal data or information as part of its functional requirements

Cyber Security means the ability or capability, to protect and/or defend information and communications systems and the information contained therein against damage, unauthorized use or modification, or exploitation.

Confidentiality means ensuring that information is not disclosed to users, processes, or devices unless they have been authorized to access the information.

DPIA Data Protection Impact Assessments

Integrity means information, an information system, or a component of a system has not been modified or destroyed in an unauthorized manner.

Issues are events which have occurred or are certain to occur which need to be managed.

Classification in the context of Information and Cyber Security, is the grouping of information based on its inherent sensitivity and the damage to Trust that would be caused if the confidentiality, integrity, or availability of that information is compromised.

Malicious Code/Malware means code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Examples of malware include viruses, Trojans, ransomware and worms.

Risk Appetite The Trust's risk appetite is the amount of risk that it is willing to accept in pursuit of its strategic objectives. Risk appetite therefore reflects the desire to optimally exploit our opportunities and minimise hazard to an acceptable level.

Controls A process put in place to provide reasonable assurance that business objectives will be achieved. It includes all measures and practices used to mitigate exposure to risks.

Security Event is a change in the everyday operations of a network or information technology service indicating that a security safeguard may have failed or a security policy may have been violated.

Security Incident is an event that may indicate that any of the Trust's systems or data have been compromised (often found by an analysis of a security event).

Security Breach means any incident that may or potentially results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.

A Data breach is a security breach in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. For example, education records or payroll data.

Personal Data breach is a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Personal Data means data relating to a living individual.

Special Categories of Personal Information refers to information relating to an individual's
(a) racial or ethnic origin, their political opinions, religious beliefs or other beliefs of a similar nature, whether they are members of a trade union) and
(b) Their physical or mental health or condition, sexual life, the commission or alleged commission by them of any offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Policy means the Information and Cyber Security Policy.

Appendix 1 – How Information and Cyber Risks Arise

The key reasons that lead to Information risks being realised include:

- Lack of ownership and accountability for information, and the processes that handle information in the Trust
- Lack of ownership and accountability for key systems within the Trust
- Inability to identify critical information and failing to protect it appropriately
- Lack of user awareness, training and education on the threats to information
- Poor Information Security culture
- Poor understanding of the regulatory requirements for dealing with personal data
- Not including security requirements in the systems development lifecycle
- Lack of investment in IT security control
- Poor control selection due to inadequate risk analysis
- Poor change control and management
- Lack of effective monitoring of the control environment
- Inability to respond swiftly to minimise the impacts of security breaches
- Poor control environments at third parties who transmit, store or process the Trusts information
- Poor user behaviour and use of IT
- Poor control over portable devices (laptops, iPads etc.), whether Trust or employee owned
- Lack of appropriate security over premises
- “Hacking” attacks, often described as ‘Cyber’ attacks. Where these use new techniques or technology (also known as ‘zero-day’ exploits), these can cause significant reputational and financial damage. Often no immediate mitigation is available.

Appendix 2- The Control Framework

The following requirements must be included and maintained as part of the Trust's framework for controlling Information and Cyber related risks:

The Management of IT and Information Assets
A management process must be implemented to ensure that only proven, reliable and approved hardware and software is used within the Trust. Essential information about hardware and software should be recorded in inventories and software licensing requirements met. Reference should be made to the Trusts Data Protection Impact Assessments (DPIA) that ensures any changes (or projects) that relate to Information Security are assessed consistently and in line with regulatory and company requirements.

Identity and Access Management
Access to information must be restricted to authorised individuals and enforced accordingly. Access should be provided on a 'least privilege' basis and withdrawn when no longer needed.

All users must be authenticated by using User IDs and passwords and, for critical systems, by strong authentication mechanisms (e.g. smartcards or tokens) before they can gain access to information.

Privileged access (i.e. access authorities in excess of those available to a general user) must be subject to additional controls, including logging and monitoring, where this is technically feasible.

Access authorities must be periodically reviewed to ensure that users still require them and that they are appropriate for their role. Privileged access authorities must be similarly reviewed, but at more frequent intervals.

Physical and Environmental Security
Physical access to environments housing critical IT facilities, computer installations, networks and computer equipment must be restricted to authorised individuals.

Such environments must be adequately protected against relevant natural hazards.

System Configuration
Systems and networks must be configured to prevent unauthorised or incorrect updates, to ensure that systems and networks operate as intended, are resilient to component failure (where justified by business criticality) and do not compromise Information Security.

System Monitoring
Critical systems must be monitored to identify and mitigate security risk events.

Management Reporting
Critical areas of the Trust and associated schools must report on the security condition of their environment to the Trust IT director/Board.

Electronic Communication
Electronic communications, including email, instant messaging and voice network facilities must be protected so the confidentiality and integrity of messages is protected in transit and the risk of misuse is minimised.

Cryptography
Cryptography should be used to protect the confidentiality of sensitive information, preserve the integrity of critical information and confirm the identity of the originator of information.

Malicious Software Protection
Protection against all types of malware must be established and maintained.

System Development
A system development methodology that includes proportionate Cyber Security requirements must be established to cover each stage of the systems development lifecycle.

Change Management
A Change Management process must be implemented on installations, networks and applications to ensure that changes are applied correctly and do not compromise Cyber Security. A DPIA must be completed for all changes

Consumer Devices
Where the Trust allows the use of personally owned consumer devices (smartphones and tablets) for work related purposes this should be supported by a documented agreement with the users and appropriate technical controls to protect business information.