The Bishop Konstant Catholic Academy Trust

Learning Communities, Inspired by Faith

Trust Information Security Policy 2019

The Bishop Konstant Catholic Academy Trust,
The Zucchi Suite, Nostell Business Estate, Nostell,
Wakefield, WF4 1AB

Telephone: 01924 802285
Email: admin@bkcat.co.uk **Website:** www.bkcat.co.uk

POLICY DOCUMENT	Trust Information Security Policy
Legislation/Category: Academy Schools	Legally Required
Lead Member of Staff:	Trust IT Manager
Approved by:	BKCAT Trust Board
Date Approved:	April 2019
Revision Date:	April 2020
Review Frequency:	1 year
Audience	All Staff

Version	Date	Author	Changes
1.1	23/5/2019	Trust IT Manager	Minor changes after review of document by committee
1.0	26/03/2019	Trust IT Manager	Starting Document and Layout.

All policies are written in line with our ethos:

Within the Bishop Konstant Catholic Academy Trust, our academies are communities where our children and young people are given a clear vision for life, a vision which is rooted in the person and teachings of Jesus Christ and which is faithful to the mission of the Catholic Church.

The Trust seeks to serve all our families (Catholic and non-Catholic alike) and to work with other partners in education for the benefit of our children and young people; we are committed to working together as academies and with the wider community for the common good. In our academies, we uphold the dignity and unique human value of every person as we strive for excellence in education; gifts and talents are shared between our academies as we aim to provide the highest standards for all our children and young people, aged 3 to 19 years throughout the Trust.

Trust Information Security Policy

Introduction

The Bishop Konstant Catholic Academy Trust (hereafter referred to as the Trust) is committed to ensuring that all personal data we process, including that of colleagues and customers, is managed appropriately and in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) (collectively referred to as "DP legislation").

The Trust is committed to ensuring that all personal data is processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Negligent or malicious non-compliance with this policy may be dealt with through the disciplinary process.

Related documents

- Trust General Data Protection Regulation (GDPR) Policy
- Trust Personal Data Security Incident Reporting Procedure

Responsibilities

- The Trust has overall responsibility for ensuring compliance with this policy and with Data Protection legislation;
- The Trust IT Manager has day-to-day responsibility for monitoring compliance with this policy, advising the organisation on information security;
- The Trust has responsibility for advising the organisation on data protection matters, in particular being consulted on new systems or business activities impacting on the organisation's use of personal data, and for receiving reports of personal data incidents for escalation as appropriate;
- Headteachers are responsible for ensuring that all systems, processes, and information assets within their Academy are compliant with this policy and with Data Protection legislation; for assisting the Trust IT Manager in their duties through providing all appropriate information and support; for ensuring that their staff are aware of their information security responsibilities;
- **All colleagues** are responsible for understanding and complying with relevant policies and procedures for securing the organisation's information assets, and for immediately reporting any event or breach affecting information assets of the organisation.

Information Security Objectives

The Information Security Objectives of the organisation are to ensure the **Confidentiality, Integrity and Availability** of all the organisation's information assets and in particular:

- Maintain business continuity through the resilience of information systems and assets, with zero significant disruption to customer services where relevant process are in place;
- To ensure appropriate levels of security with GDPR and Data Protection for all personal data held by the organisation;
- Raise and maintain staff awareness of information security responsibilities, by supplying training as appropriate.

Accountability and governance

Risk management – The Trust maintain an Information Risk Management regime. The Trust will maintain a corporate information risk register and ensure there is ongoing assessment of information risk to inform our security posture and investment.

Acquisition and development – All procurement processes for new or upgraded applications or ICT system must include appropriate security functionality and design requirements within the specifications must be risk assessed by the Trust IT Manager. In addition, if they are to contain personal data, the Data Protection Officer must be consulted for a potential Data Protection Impact Assessment.

Information security controls – technical

The organisation will maintain appropriate technical security controls including but not limited to the following:

Firewalls – The Trust will configure and use a firewall to protect our network and all our devices where appropriate;

Configuration – The Trust will configure all our devices and software to the most secure settings commensurate with the business purpose;

Access –The Trust will control access to our data through user accounts and ensure that administration privileges are only given to those that need them;

Malware – The Trust will protect our data through applying and maintaining appropriate anti-malware protection;

Patching – The Trust will keep our devices, software and apps up to date where possible;

Back-up – The Trust will ensure business continuity through regular back-up of all corporate data and the testing of recovery from back-up systems;

Encryption – The Trust will ensure that mobile devices and removable media where possible are encrypted and that our email system supports encryption of data in transit;

Testing – The Trust will ensure that security controls are monitored and regularly tested.

Information security controls – users

All members of staff will apply appropriate security controls including:

Clear desk – All records, portable devices and removable media will be locked away when not in use as required by the Trust's clear desk policy;

Password – Use strong passwords for access to organisation data and protect that password from disclosure or sharing;

Systems – To report using the relevant and available methods on out of date systems or failed updates;

Authorised use – Only hold organisational information and data on authorised applications, devices and systems and do not attempt to access or use data or systems not required for your role;

Phishing and spam – Be alert to malicious emails and do not open spam emails or links or attachments from unknown sources;

Report – Report all incidents, near misses or identified risks immediately following the Trust Personal Data Security Incident Reporting Procedure.

In addition, personal data breaches must be reported to the Data Protection Co-ordinator and the Data Protection Officer.

Information security incident response

The Data Protection Officer will co-ordinate our response to information security incidents, escalating these as appropriate and, for events with significant business impact, with the support of the Trust IT Manager or other staff as required. Our incident response will seek to:

- Emphasise rapid business recovery;
- Restore security to our data and systems;
- Mitigate the impact of the incident;
- Gather information and evidence on the causes of the incident;
- Ensure lessons are learned, recorded and acted on.

Monitoring and Review of this Policy

The Trust IT Manager shall be responsible for reviewing this policy from time to time to ensure that it meets legal requirements and reflects best practice.