



St. Cuthbert's
Roman Catholic High School

WHOLE SCHOOL POLICY & PROCEDURES

DATA PROTECTION



Mission Statement

*'The Lord God requires of us that we should help others whenever we can,
always make the right choices and be the best that we can be in everything that we do'.*

Policy: Data Protection Policy		
Type: School Policy	Website: Yes	Author: J Ward
Approved: July 2020	Next Review: September 2022	
Frequency: 2 Yearly	Delegated: Governors - Full	
Notes:		

Document Control

Publication Date	25 th May 2020
Related Legislation / Applicable Section of Legislation	Data Protection Act 2018 General Data Protection Regulation (GDPR) Digital Economy Act 2017 Human Rights Act 1998 Freedom of Information Act 2000 The Privacy and Electronic Communications Regulations EU e-Privacy Directive
Related Policies, Strategies, Guideline Documents	
Replaces	Data Protection Policy 2017
Policy Owner (Name/Position)	Mr J Ward – IT Manager
Policy Author (Name/Position)	Mr J Ward – IT Manager

Review of Policy

Last Review Date	2020
Review undertaken by	Mr J Ward
Next Review Date	This policy will be review following the enactment of the Data Protection Bill into law

Document Approvals

This document requires the following approvals.

Name	Title	Date of Approval	Version Number

CONTENTS:

1. Introduction.....	Page 6
2. Policy.....	Page 7
3. Monitoring Compliance	Page 10
4. Policy Review.....	Page 10
5. Call recording policy.....	Page 10
6. Glossary and Appendix	Page 11

Executive Summary

Information is a vital asset and resource, both in terms of the management of individuals and the efficient management of services and its support. It plays a key part in governance, service planning and performance management.

- Data Protection & Privacy
- Data Quality
- Information Security
- Information Sharing
- Records Management

Implementation of this policy will contribute significantly towards assuring the Schools stakeholders that information is being processed in compliance with legislation and School Policies. This policy will support the provision of high-quality services by promoting the effective and appropriate use of information.

The governing body has overall responsibility for ensuring that the School complies with all relevant data protection obligations. The headteacher acts as the representative of the governing body on a day-to-day basis.

1. Introduction

The School is committed to protecting the privacy of individuals and handles all information in a manner that complies with relevant legislation & codes of practice including but not limited to the Data Protection Act 2018, General Data Protection Regulation, Digital Economy Act 2017, Human Rights Act 1998, Freedom of Information Act 2000 and common law duty of confidentiality. The School has established this policy to support that commitment.

In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record. Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

The Policy applies to all information held on paper or in electronic format including recorded information e.g. CCTV, voice recordings.

Everyone managing and handling information, particularly personal information, needs to understand their responsibilities in complying with the legislation & codes of practice. It is the personal responsibility of:

- All employees of the School
- All employees and agents of other organisations who directly or indirectly support or are procured by the School, including all temporary and agency staff directly or indirectly employed by the School
- Those engaged on interim contractual arrangements or agency contracts working on behalf of the School
- Suppliers and Data Processors of the School

The School recognises that there are risks associated with managing information in order to meet legislative and other requirements. This policy is intended to facilitate compliance & reduce risks regardless of how data is processed, and all staff should be aware of its content and requirements. Several guidance documents and information have been developed to support the application of this policy and the management of risk.

The School has a clear commitment to ensuring that all staff have access to appropriate training or guidance. Managers must ensure that those staff managing and handling personal & other information are adequately trained regarding the requirements of this and all other Information Governance Policies.

The School will have processes in place to manage Induction, Refresher and Subject Area Training for all staff.

The School has implemented an awareness raising and communication process for Information Governance to keep staff up to date with new areas, policy updates and training requirements.

The School has arrangements in place to manage all legislative requirements including procedures to manage requests made on your own 'individual rights' e.g. subject access requests.

The School has appointed the following roles to provide direction and oversight:

Senior Information Risk Owner (SIRO) - fosters a culture for protecting information and data and provides a focal point for managing information risk and information assurance.

Data Protection Officer – is responsible for informing and advising the School of its obligations under data protection and privacy legislation and monitoring compliance. The DPO has a list of statutory tasks and has due regard to risk considering the nature, scope, context and purposes of processing.

2. Policy

2.1 Data Protection

The Data Protection Act 2018 and General Data Protection Regulation state how an organisation can use (process) personal information about individuals. The School has established this policy to ensure it meets legal requirements and has clear procedures and arrangements in place to manage compliance across all areas. Information will be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The School is required to protect the rights and freedoms of individuals, their right to protection of their personal data. This is not an absolute right and must be balanced against other fundamental rights and be considered alongside the principles of proportionality and necessity.

The School has a Corporate Privacy Notice in place. The Privacy Notice ensures that individuals are aware of how the School use their personal information. This is supported in other ways to tell customers how their information will be used e.g. verbally, forms and other corporate information such as leaflets. The School also uses layered privacy notices, where necessary, to provide topic specific information where this is felt to be beneficial.

In order to operate efficiently, the School must collect and use information about people with whom it works for a variety of different purposes depending upon the type of service it is providing. These are the specified, explicit and legitimate purposes referred to in legislation. These may include pupils and parents/guardians, members of the public, current, past and prospective employees and suppliers. The School will ensure that information is not further processed in a manner that is incompatible with those purposes and that the information collected is adequate, relevant and necessary for the purpose it is collected.

In addition, the school may be enabled required by law to collect and use information in order to carry out its functions as may be required by law and as directed by central government.

Whilst the data that the School holds can be very useful in delivering & improving services, it also has a duty of care in respect of its handling and controlling access to this data especially in relation to personal, special category and criminal conviction and offence data.

The School will promote the use of Data Privacy Impact Assessments or similar arrangements to assist in identifying and minimising the privacy risks of new or existing projects, practices or policies.

The policy supports the rights of individuals to be informed of the risks and safeguards in place to protect their information and how to exercise their rights in relation to that information. These include the right to be informed, right of access to data, right to portability and the right to object to processing.

It meets the requirements of the [Protection of Freedoms Act 2012](#) in relation to processing biometric data.

2.2 Information Security

Information security is the practice of protecting information from unauthorised access or use, modification, accidental loss or destruction. The School has effective safeguards in place to make sure that personal and other information is kept securely and does not fall into the wrong hands. The School has clear procedures and arrangements to manage the human and technical elements of Information Security.

The School will maintain & protect all information assets both owned or used by the School to a high standard of confidentiality, integrity and availability. The School will ensure that information assets and hardware that are no longer needed are disposed of securely in line with industry standards.

Important information assets will include paper records stored on or off site, computers, mobile phones, emails, data files, software, recorded information e.g. CCTV, voice recordings.

The School will maintain an Information Asset Register to track, manage and dispose of these assets in line with legislative requirements & School Policy.

The School will ensure that any security incidents that occur are managed in line with current procedures for Information Security Breaches. It is the duty of all staff and other parties accessing or processing School data to immediately report any actual or suspected breaches in information security in line with School procedure.

2.3 Data Quality

Consistent, high-quality, timely and comprehensive information is vital to support good decision-making, protect vulnerable people, improve outcomes for users & services and reduce unnecessary work. The School will ensure that information collected is accurate and, where necessary, kept up to date and will respond to requests from customers to correct the accuracy of their information.

Data quality is the responsibility of every member of staff collecting data or entering, extracting or analysing data from any of the School's information systems. All staff should know how their day-to-day job contributes information needed to deliver services and how lapses can affect, the School's reputation, financial penalties/fines, performance management, service delivery (particularly to vulnerable people) & the allocation of funding to the School.

2.4 Records Management

The School will ensure appropriate arrangements are in place for the care and management of its records to enable the school to meet its legal and regulatory requirements. School records will be accurate and accessible, giving a fair and truthful representation of the work and processes undertaken.

Effective records management is an integral part of achieving corporate goals and meeting legal and regulatory obligations. The School will manage records throughout their lifecycle from creation to eventual disposal thus ensuring that records are complete, authentic, trustworthy and secure and are available when needed. The School has clear procedures and arrangements for handling records including a Retention Schedule outlining how long we retain certain types of information to make these decisions. We will only keep your personal information for as long as the law specifies or where the law does not specify this, for the length of time determined by our business requirements.

The School recognises that there are risks associated with managing records in order to meet legislative requirements. Non-compliance with this policy could have a significant effect on the efficient operation of the School and may result in financial loss and an inability to provide necessary services and information to customers. This policy is intended to mitigate those risks.

2.5 Information Sharing

The School will ensure that it is mindful of the legal basis for sharing data including personal data across its functions and with external partners especially in relation to non-routine data sharing or new projects where the sharing process changes in terms of purpose, parties, type of data, or means of sharing i.e. new computer systems etc. (the why, who what and how).

The School will ensure that in all cases where consent of an individual is required that the requisite privacy notices are given to individuals to enable them actively to give informed consent.

The School will use a range of Contractual terms, Data Processor and Information Sharing Agreements as may be appropriate to manage the sharing and disclosure of information to bodies within and outside the School.

Data, Privacy, Impact Assessments will be used, when required, at the outset for new projects, plans or policies that require the sharing of data to assess and mitigate risks identified and support good information sharing practice.

3. Monitoring Compliance and Effectiveness of the Policy Document

This policy will be subject to compliance audits instigated and overseen by the Data Protection Officer.

Information Governance is viewed seriously by the School. Any breach of this Policy and other associated requirements, will be considered and investigated under both the Schools Disciplinary Procedure and Information Security Breach Procedure or restricted to one of the two procedures. Dependent upon the seriousness of the allegations and outcome of investigations, and employees should be aware that this may result in disciplinary action an outcome of which may have serious consequences for an employee's continued employment.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s). Sections 170 – 173 of the Data Protection Act 2018 cover offences under the Act which include obtaining, disclosing or retaining personal data without the consent of the data controller. Examples could include, misusing council/school systems to source information for personal use, 'hacking' of council systems, selling personal data held on a Council/school system.

4. Policy Review Date

The policy shall be reviewed on a bi-annual basis but include any relevant regulation changes as they become law.

5. Call recording policy

Overview

The purpose of this document is to outline the roles and responsibilities of St Cuthbert's RC High School in its duty under the data protection act 1998 and the Telecommunications Regulations 1999.

5.1 What can be monitored?

The school can if it deems necessary record a conversation of the following:

1. Establishing the existence of facts
2. Ascertaining compliance with regulatory or self-regulatory practices or procedures
3. Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system
4. Preventing or detecting crime
5. Investigating or detecting unauthorized use of the business telecoms systems
6. Ensuring the effective operation of the system
7. Training of staff
8. Quality control

5.2 Method of recording

Data will be recorded digitally and kept for a period of no longer than 30 days from the time of the recording, after this point the recording shall be destroyed unless it has been deemed necessary to keep the recording for legal purposes.

If there has been a request for the recording to be kept longer than this the recording must be signed over to the proper authorities and responsibility for the destruction of the recording will be transferred to the 3rd party.

Only official 3rd parties will be able to request a copy of said recordings and this must be placed in writing to the data controller of St Cuthbert's RC within the 30-day validity period of the recording.

Recordings are not encrypted and are stored on user's local voicemail, they cannot be used as evidence in a UK court as the recordings are not encrypted, tamper proof or timestamped.

5.3 Informing relevant parties of recording/monitoring

It is not necessary to gain consent from participants in a telephone call before commencing recording, monitoring or Intercepting.

However, all reasonable efforts must be taken to inform all parties of the intent to record or monitor. This is generally achieved via information contained in advertisements, letterheads or within terms and conditions.

It is also acknowledged that in certain circumstances it may not be appropriate to publicise the existence of recording equipment externally (i.e. monitoring a switchboard for bomb threats) and provision is made for this within the guidelines.

However, the recent European Convention on Human Rights judgment based on the principle that "everyone has the right to respect for his private and family life, his home and his correspondence" must be borne in mind.

It may, therefore, not be enough to warn employees external parties that their calls may be monitored because it is not reasonable to assume that people at work will never make or receive calls touching on personal and or domestic matters. This means there must be some way for employees to make and receive personal calls that will not be monitored or recorded in the workplace.

As with external parties' employers have an obligation to make all reasonable efforts to make internal employees aware that calls may be monitored or recorded. If this is regularly carried out it can be taken as implied consent and removes the expectation of privacy. Although not a strict legal requirement, it is certainly good practice to make staff aware of why their calls may be recorded. This will offer a higher degree of protection in case of a legal challenge.

6 Reference

<http://www.opsi.gov.uk/si/si2000/20002699.htm>

http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_3#pt1-ch1-pb4-l1g16

<http://www.legislation.gov.uk/ukpga/1998/29/contents>

Appendix A – Data Protection Principles

Principle
5 (1)(a) processed lawfully, fairly and in a transparent manner in relation to the data subject
5 (1)(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
5 (1)(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
5 (1) (d) accurate and, where necessary, kept up to date
5 (1) (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
5 (1) (f) processed in a manner that ensures appropriate security of the personal data

6. Glossary of Terms

Term	Meaning
Data Protection Act 1998	Historic legislation governing the protection of personal data and privacy in the UK.
Data Protection Act 2018	The main pieces of legislation that govern the protection of personal data and privacy in the UK.
General Data Protection Regulation	
Digital Economy Act 2017	Legislation allowing greater sharing and use of data across the public sector for purposes such as improving wellbeing and welfare, aiding research and combating fraud.
Human Rights Act 1998	Article 8 covers the right to respect for family, private life, home and correspondence and makes it unlawful for any public body to interfere with that right.
Data Privacy Impact Assessments	A tool to identify and address privacy risks for projects or changes in practice. Under GDPR, some DPIA need to be approved by the Information Commissioners Office.
Freedom of Information Act 2000	The main piece of legislation providing public access to (non-personal) information held by public authorities.
The Privacy and Electronic Communications Regulations	Sit alongside the Data Protection Act. They give people more privacy in relation to electronic communications.