St Bede's Catholic Primary School

Data Breach Policy

Introduction

St Bede's Catholic Primary School holds processes and shares a large amount of personal data, a valuable asset that needs to be protected.

Every care is taken to protect personal data from incidents (either accidental or deliberate) to avoid a data protection breach that could compromise security.

Compromise of information, confidentiality, integrity, or availability may result in harm to individuals, reputational damage. Detrimental effect on service provisions, legislative non-compliance, and / or financial costs.

Purpose

St Bede's RC Primary School is obliged under the Data Protection Act (DPA) and the General Data Protection Regulation:

- Have in place a framework designed to ensure security of all personal data during its lifecycle, including clear lines of responsibility.

This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the school.

Scope

The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what remedial action is necessary to secure personal data and prevent further breaches.

- This policy relates to all personal and special category data held by the school, regardless of format
- This policy applies to all staff and pupils and contractors at the school. This includes teaching students, temporary, casual, agency staff, suppliers and data processors working for or on behalf of the school.

A personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This will include breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

It is a security incident that has affected the confidentiality, integrity or availability of personal data. Whenever a security incident takes place, it should be quickly established whether a personal data breach has occurred and, if so, promptly take steps to address it, including informing the ICO if required.

The ICO must be informed if the breach has resulted in a risk to people's rights and freedoms; if this is unlikely then it does not have to be reported. However, if the breach has not been reported then the school should be able to justify this decision.

In assessing if a data breach has created a risk to people's rights and freedoms then Recital 85 of the GDPR should be consulted.

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

There are several courses of action that can be followed following a data breach. Advice may be given to the individual staff member specifically and/or to school staff in general. This may also result in additional training for an individual, team or whole staff. In the most serious cases and/or when there is evidence to suggest disregard for procedures then this could result in staff receiving a verbal warning, a written warning or potentially dismissal

Data Breach Process

1. Data Breach reported to either head teacher or school data protection officer. Whichever is informed, they will inform the other with immediate effect.

2. Immediate action taken to contain the breach.

3. Begin completion of the data breach document log by Data Protection Officer.

4. Any actions from data breach document log carried out.

5. Chair of Governors to be informed in a timely manner.

6. Completed data breach document log agreed by both Head Teacher and Data Protection Officer and copies kept by both.

Reviewed and ratified by Governors:

Date: ……

Signed: …….. (Chair of LGC)

Date to be reviewed: ……

APPENDIX 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify your Head Teacher of it immediately

and inform Bryan Chapman - Chapman Data and Information Services Ltd dpo@chapmandis.co.uk

Section 1: Notification of Data Security Breach	**To be completed by Head Teacher reporting incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Lead Investigation Officer in consultation with the Head Teacher if appropriate IT where applicable**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the St Bede's RC Primary School or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data • Special Category data (as defined in the Data Protection Act) relating to a living, identifiable individual's a) Racial or ethnic origin; b) Political opinions or religious or philosophical beliefs; c) Membership of a trade union; d) Physical or mental health or condition or sexual life; e) Biometric data	
• Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	

• Personal information relating to parents, staff and children	
• Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
• Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals	
• Security information that would compromise the safety of individuals if disclosed.	

Section 3: Action taken	**To be completed by Data Protection Officer and/or Lead Investigation Officer**
Incident number	**e.g. year/001**
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to Data Protection Officer and Lead Officer on (date):	
Reported to other internal stakeholders (details, dates):	
For use of Data Protection Officer and/or Lead Officer:	
Notification to ICO	**YES/NO If YES, notified on:** **Details:**
Notification to data subjects	**YES/NO If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder	**YES/NO If YES, notified on:** **Details:**