Data Breach Policy

Date adopted: *19/06/18* Next review date: *19/06/20*

Responsible committee	Resources
Date approved by committee	19/06/18
Date ratified by FGB (if required)	n/a
Description of changes from the model policy (if any)	

1.0 Introduction

1.1 St Michael's Church School holds, processes, and shares personal data, a valuable asset that needs to be suitably protected.

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

1.3 Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

2.0 Purpose

2.1 St Michael's Church School is obliged under the General Data Protection Regulations 2018 to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

2.2 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 St Michael's Church School.

3.0 Scope

3.1 This Policy relates to all personal and sensitive data held or processed by St Michael's Church School regardless of format.

3.2 This Policy applies to all staff, unpaid, employed or contracted including Governors and students at the School. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the School.

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

4.0 Definition/Type of Breach

4.1 For the purpose of this Policy, data security breaches include both confirmed and suspected incidents.

4.2 An incident in the context of this Policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately and has caused or has the potential to cause damage to the School's information assets and/or reputation.

4.3 An incident includes but is not restricted to, the following:

- 4.3.1 Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)
- 4.3.2 Equipment theft or failure
- 4.3.3 Unauthorised use of, access to or modification of data or information systems
- 4.3.4 Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- 4.3.5 Unauthorised disclosure of sensitive/confidential data
- 4.3.6 Website defacement]
- 4.3.7 Hacking attack

4.3.8 Unforeseen circumstances such as a fire or flood
4.3.9 Human error
4.3.10 'Blagging' offences where information is obtained by deceiving the organisation who hold it.

5.0 Reporting an Incident

5.1 Any individual who accesses, uses or manages the School information is responsible for reporting a data breach or information security incidents immediately to the Data Controller, Mrs Stephanie Hibbitt

5.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

5.3 The report should be made using the report template in Appendix A to include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. These forms are available from the Staff area on the server.

5.4 All staff should be aware that any significant breach of the GDPR & Data Protection Bill (when enforced) may result in the School's Disciplinary Procedures being instigated.

6.0 Containment of Recovery

6.1 The Data Controller will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

6.2 The Data Controller will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

6.3 The Data Controller will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

6.4 Advice from experts across the School may be sought in resolving the incident promptly.

6.5 The Data Controller will determine the suitable course of action to be taken to ensure a resolution to the incident.

7.0 Investigation and Risk Assessment

7.1 An investigation will be undertaken by the Data Controller immediately and wherever possible within 24 hours of the breach being discovered/reported.

7.2 The Data Controller will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

7.3 The investigation will need to take into account the following:

7.3.1 The type of data involved
7.3.2 The protections are in place (e.g. encryptions)
7.3.3 What has happened to the data, has it been lost or stolen
7.3.4 Its sensitivity
7.3.5 Whether the data could be put to any illegal or inappropriate use
7.3.6 Who the individuals are, number of individuals and the potential effects on those data subject(s)
7.3.7 Whether there are wider consequences to the breach

8.0 Notification

8.1 The Headteacher and Local Authority representative will determine who needs to be notified of the breach.

8.2 Every incident will be assessed on a case by case basis; however, the following will need to be considered:

8.2.1 Whether there are any legal/contractual notification requirements;

8.2.2 Whether notification would assist the individual affected – could they act on the information to mitigate risk?

8.2.3 Whether notification would help prevent the unauthorised or unlawful use of personal data?

8.2.4 Would notification help the School meet its obligations under the seventh data protection principle;

8.2.5 If a large number of people are affected, or there are very serious consequences, whether the Information Commissioner's Office (ICO) should be notified. The ICO will only be notified if personal data is involved. Guidance on when and how to notify ICO is available from their website at: https://ico.org.uk/for-organisations/report-a-breach/

8.2.6 The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

8.3 Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the School for further information or to ask questions on what has occurred.

8.4 The Data Controller must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

8.5 The Data Controller will consider whether the Local Authority should be informed regarding a press release and to be ready to handle any incoming press enquiries.

8.6 All actions must be recorded by the Headteacher.

9.0 Evaluation and Response

9.1 Once the initial incident is contained, the Data Controller will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

9.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

9.3 The review will consider:

9.3.1 Where and how personal data is held and where and how it is stored

9.3.2 Where the biggest risks lie, and will identify any further potential weak points within its existing measures
9.3.3 Whether methods of transmission are secure; sharing minimum amount of data necessary
9.3.4 Identifying weak points within existing security measures
9.3.5 Staff awareness
9.3.6 Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security

9.4 If deemed necessary recommend any changes to systems, policies and procedures.

APPENDIX 1
DATA BREACH REPORT FORM

Section 1: Notification of Data Security Breach	*To be completed by person 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 Controller	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	
Section 2: Assessment of Severity	**To be completed by the DPO in consultation with the School Business Manager and Headteacher**

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 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	
● Sensitive personal data (as defined in the GDPR)	
● 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 vulnerable adults 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.	
Headteacher to consider whether it should be escalated to the Governing Body	

Section 3: Action taken	**To be completed by Data Protection Officer**
Incident number	
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 on (date):	
Reported to other internal stakeholders (details, dates):	
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:**