All Saints Church School
A Bath and Wells Academy

Data Protection – Data Breach Policy

1. Introduction

All Saints Church School issues this policy to meet the requirements incumbent upon them under the General Data Protection Regulation (GDPR) 2016 and Data Protection Act 2018 for the handling of personal data in its role as a data controller and data processor, such personal data is a valuable asset and needs to be suitably protected.

Appropriate measures are implemented to protect personal data from incidents (either deliberately or accidently) to avoid a data protection breach that could compromise security.

A data breach is defined as the compromise of information's confidentiality, integrity, or availability which may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

2. Scope

This policy applies to all employees of All Saints Church School including contract, agency and temporary staff, Governors volunteers and employees of partner organisations working for All Saints Church School.

3. Roles and Responsibilities

All stakeholders which include staff, contractors, consultants, suppliers, volunteers, governors and trustees must:

a) Be familiar with this policy and other relevant policies and procedures including, but not limited to:
   i. Data Protection Policy
   ii. Special Categories of Personal Data Policy
   iii. Data Breach Policy
   iv. Data Retention Policy (IRMS Toolkit)
b) Play an active role in protecting information in their work
c) Read and act on any training and awareness, and communications regarding information security and ask for clarification if these are not understood
d) Take care when handling information to ensure it is not disclosed to those without the need to know or are not approved
e) Report any breaches, near misses, or incidents to the organisation via the organisation's Data Breach Policy and procedures

Governors and Senior Leaders are required to:

a) Approve this policy

b) Actively promote a culture of privacy and security
c) Ensure security and privacy is considered throughout the development of any new service, process or product
d) Cascade any relevant communications regarding information security
e) Ensure Information Owners and Information Custodians are assigned for its critical information assets

Ultimately this group are accountable for the organisation's information, therefore there may be other elements that this cohort deliver as part of their roles.

Data Protection Officer is required to:

a) Monitor compliance with Data Protection Law and this policy, reporting this to the Local Governing Board annually.
b) Assist the organisation with any Data Protection Impact Assessment which could include recommending controls to reduce risk
c) Assist the organisation with any queries they have regarding data protection

4. Data Breaches

For the purposes of this policy data breaches will include both suspected and confirmed incidents.

An incident can include, but is not limited to:

- Loss or theft of confidential or personal data or special category personal data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*
- Equipment failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of personal data or special category personal / confidential data *(e.g. login details, emails to the wrong recipient, not using BCC, post to the wrong address)*
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error
- Breaches of policy such as
    - Server Room door left open
    - Filing cabinets left unlocked
    - Temporary loss / misplacement of confidential or personal data or special category personal data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*

Near misses can include, but are not limited to, scenarios such as emails sent to the wrong recipient where a non-delivery report bounces back.

5. Reporting

The quick response to a suspected or actual data breach is key. All consumers in scope of this policy have a responsibility to report a suspected or actual data breach. If this is discovered or occurs out of hours then this should be reported as soon as practically possible. This should be done through the completion of the reporting form in Appendix 1, which is sent to office@allsaints.bwmat.org who will liaise with its Data Protection Officer (i-west).

6. Security Incident Management (SIM)

The organisation's lead officer (Head Teacher) shall complete the following phases of SIM (which are detailed in Appendix 2) with advice from its Data Protection Officer:

a) **Preparation** – the organisation will understand its environment and be able to access the necessary resources in times of incidents. It will also ensure its staff are aware of how to identify and report breaches

b) **Identification** – the organisation will determine whether there has been a breach, or a near miss, it will also assess the scope of the breach, and the sensitivity on a risk basis.

c) **Containment & Eradication** – the organisation will take immediate appropriate steps to minimise the effect of the breach. It will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause, and will establish who may need to be notified as part of the initial containment and will inform the police and other enforcement bodies where appropriate.

d) **Recovery** – the organisation will determine the suitable course of action to be taken to ensure a resolution to the incident. This may include re-establishing systems to normal operations, possibly via reinstall or restore from backup.

e) **Wrap Up / Learning from Experience (LfE)** – an assessment will be made on the likely distress on any affected data subjects. This will then form the decision on whether to report this to the regulator (ICO) (reporting will be completed by i-west on behalf of All Saints Church School) which must be reported within 72 hours, and to the affected data subjects which must be done without undue delay. The BWMAT's central team may also be notified to handle any queries and release statements.

A review of existing controls will be undertaken to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. All Saints Church School will use Security Incident Management (SIM): Record of work to review these controls.

The review will consider:

- Whether policy controls are sufficient
- Whether training and awareness can be amended and/or improved
- Where and how personal data is held and where and how it is stored
- Where the biggest risks are apparent and any additional mitigations
- Whether methods of transmission are secure
- Whether any data sharing is necessary

If necessary a report recommending any changes to systems, policies and procedures will be considered by the Head Teacher and BWMAT central team. This will include the decision on whether to report to the regulator and affected data subjects in conjunction with the DPO.

Phases (b) to (e) will form part of the investigation process. This process should commence immediately and wherever possible within 24 hours of the breach being discovered or reported.

7. Monitoring and compliance

Compliance with this policy shall be monitored through an annual review process. This will be agreed with the Data Protection Officer, and compliance will be reported to the Head Teacher. Local Governing Body and BWMAT central team.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation, in consultation with senior management, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

Review this Policy upon;
Change of Data Protection Officer,
Change of Legislation

Appendix 1 – Data Incident Reporting Form

1. About the incident	
Date and time of incident	
Where did the incident occur?	
Date (and time where possible) of notification to the organisation	*If there was any delay in reporting the incident, please explain why this was*
Who notified us of the incident?	
Describe the incident in as much detail as possible, including dates, what happened, when, how and why?	*Include names of staff and data subject(s). Identifying information will be anonymised for any reporting purposes.*
2. Recovery of the data	
What have you done to contain the incident?	*eg limiting the initial damage, notifying the police of theft, providing support to affected data subjects*
Please provide details of how you have recovered or attempted to recover the data, and when	*Consider collecting the lost data, rather than relying on an unintended recipient to dispose of it*
3. About the affected people (the data subjects)	
How many individuals' data has been disclosed?	
Are the affected individuals aware of the incident, and if so, what was their reaction?	
When and how were they made aware / informed?	
Have any of the affected individuals made a complaint about the incident?	
Are there any potential consequences and / or adverse effects on the individuals? What steps have been taken / planned to mitigate the effect?	
Your name and contact details:	

Appendix 2 - Security Incident Management (SIM): Record of work

This document provides the documented evidence and audit trail of a reported information security incident. It is designed to operate alongside the organisation's Data Protection Policy, and Data Breach Policy.

This form is to be completed by the Incident Handler(s) (Head Teacher) in the organisation.

The incident may require additional input and support from the organisation's Data Protection Officer, ICT, and potentially other specialist bodies (e.g. National Cyber Security Centre – NCSC)

Incident No:	
Severity (H, M, L):	
Basis for initial severity rating:	
Incident Handler(s):	
Date reported to organisation:	
By whom:	
Date reported to Incident handler:	
By whom:	
Date incident occurred:	
Senior Management notified (date):	

Summary of breach:	

Incident Response Phase	Evidence/Actions Taken
1. Preparation Gather and learn the necessary tools, become familiar with your environment	• Necessary staff trained on incident handling and incident response • Policy, Procedures & Guidance • Network Diagrams are held by ICT • The Record of Processing Activities (RoPA) will provide details of data, owners, custodians, and third parties – link to the RoPA • ICT also record event logs and hold logs on other systems (e.g. emails, firewalls etc) • Key contacts: office@allsaints.bwmat.org
2. Identification Detect the incident – Is it an incident (breach of policy), a near miss, or a data breach? Determine its scope, and involve the appropriate parties	
3. Containment Contain the incident to minimize its effect on other IT resources	
4. Eradication Eliminate the affected elements e.g. remove the malware and scan for anything remaining	
5. Recovery Restore the system to normal operations, possibly via reinstall or backup.	
6. Wrap Up Document the lessons learned and	

actions to reduce the risk of the incident/breach/near miss re-occurring Document the decision to report to both the affected data subjects and the ICO.	
	If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay **Decision to report to Data subjects** - Yes / No Based on: Officer: Signed: Date:
	Establish the likelihood and severity of the resulting risk to people's rights and freedoms - 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 **Decision to report to ICO** - Yes / No Based on: Officer: Signed: Date: