THE SAINTS FEDERATION

GDPR - Data Protection Incidents Policy Procedure

Document Control

Organisation	The Saints' Federation All Saints' Church in Wales Primary School St David's Church in Wales Primary School St Mellon's Church in Wales Primary School
Title	GDPR Policy - Data Protection Incidents Policy & Procedure
Author	Schools Information Governance Support Officer on behalf of the Data Protection Officer
Owner	Executive Head Teacher and Governing Body
Protective Marking	NOT PROTECTIVELY MARKED
Review date	3 years or sooner is needed

Revision History

Revision Date	Revision	Previous Version	Description of Revision
March 24	1.0		
April 26			Name change to include St Mellons as part of the Saint's Federation

Signed by chair of governors on behalf of the governing body ……

Signed by the Headteacher: ……

Date approved: ……(by full governing body)

Date of review: ……

City of Cardiff Council

Data Protection Incidents Policy & Procedure

Data Protection Incidents Policy & Procedure

1 Introduction

1.1 The Saints Federation is legally required under the Data Protection legislation to ensure the security and confidentiality of the information/data it processes on behalf of its clients and employees.

1.2 Sometimes a loss of data may occur because this information/data is accidentally disclosed to unauthorised persons or, lost due to a fire or flood or, stolen as result of a targeted attack or the theft of a mobile computer devic**e.**

2 Legislation

2.1 The Saints Federation has an obligation to abide by all relevant legislation and European directives, including the:

The Data Protection Act 2018

The UK General Data Protection Regulation (UK GDPR) Human Rights Act (1998)

Privacy and Electronic Communications Regulations (2003)

3 Responsibilities

3.1 The Data Protection Officer maintains overall responsibility for ensuring compliance with this procedure, including coordinating and managing the response to any reported incident, documentation of all steps taken, evidence collection, and closing out the Event, including overseeing any recommendation/actions as a result of the breach.

3.2 All employees have a responsibility to be aware of potential Security Incidents as defined in this Policy and are required to report all incidents, both actual and suspected.

3.3 All Incidents must be reported to the Data Protection Officer via

DataLoss@cardiff.gov.uk within 24 hours. Where an incident occurs over a weekend, which is not classed as a working day, such incidents must be reported no later than 12 noon on the next working day.

3.4 Once becoming aware of an Incident, failure to report it may result in disciplinary action. Reporting should be via the Data Protection Incident Report Form at Appendix 1 of this Policy. It should be emailed to DataLoss@cardiff.gov.uk Staff and service areas themselves must not investigate what appears to be an incident.

3.5 The Data Protection Officer may in appropriate cases authorise relevant officers to conduct such investigations. In such cases reports into such incidents must be carried out immediately to ensure that any necessary action(s) is promptly taken with the final report issued to the Data Protection Officer

3.5 Technical staff and other relevant personnel are required to fully support the Data Protection Officer or staff as designated by the Data Protection Officer, in dealing with an incident.

4 Data Protection Incidents

4.1 A Data Protection Incident is a situation where The Saints Federation has lost control of the processing of data which contains personal and or confidential information which could result in distress/harm to the individuals (Data Subjects) whose data has been compromised or affect the commercial interests of third party organisations. Further details of types of data are specified in The Saints Federation's Data Protection Policy & Procedure.

4.2 Examples of Data Protection incidents would include loss of paper based records which contain personal/confidential information of third party individuals, including citizens, businesses, or employees, this also includes commercially sensitive information (including contracts). Other typical examples include loss of control of documents containing the above information sent to third party individuals or internally, this would include emails sent to incorrect recipients or to generic mailboxes, or faxes sent to the incorrect number.

4.3 Any complaints from a member of the public or an employee that they believe that their data may have been breached, or their rights of privacy have not been kept must be reported immediately to the Information Governance Team via DataLoss@cardiff.gov.uk

4.4 Loss of data can also occur through the loss of The Saints Federation Assets such as laptops, storage devices, mobile phones etc. Losses of this nature must be reported through the Asset Loss Procedure to the Service Desk (ServiceDesk@cardiff.gov.uk). The loss will be brought to the attention of the Information Governance Team who will then require further information to determine if any personal/confidential data has been compromised. This will be done using the Asset Loss – Personal Data Evaluation Form. (Appendix 2)

4.5 Any individual who becomes aware of an actual, suspected or potential Data Protection Incident must complete the Data Protection Incident report form (see

Appendix 1), forward it to DataLoss@cardiff.gov.uk AND report it immediately to their line manager / supervisor.

4.6 Where an employee is under investigation for accessing or obtaining of The Saints Federation data which does not form part of their role or where there is evidence to suggest that a member of staff has illegally processed and passed data onto a third party, these must be dealt with through normal disciplinary channels, with assistance provided by the Information Governance team and Audit. Where necessary the Information Governance team will provide statements informing the disciplinary panel of the Council's and employees statutory responsibilities under Data Protection legislation. In these instances, consideration must be given to the Council's Fraud, Bribery and Corruption Policy and the Council's Audit team should be consulted.

4.7 Where a result of an investigation and/or disciplinary action is that a Data Protection offence has occurred as listed in Appendix 5, the Data Protection Officer will report the incident to the ICO and Police and work in line with the The Saints Federation's Procedure for Dealing with Police involvement in staff disciplinary cases.

5 Management of Reported Incidents

5.1 The Data Protection Officer, on behalf of the Senior Information Risk Owner

(SIRO), will log all incidents immediately and will log the progress of an investigation, including the collection and securing of any relevant evidence as the investigation progresses.

5.2 Any information gathered during the course of an investigation is treated as potential evidence in a disciplinary, criminal or civil action. If the likelihood of legal, civil or criminal action is established, the involvement of police and legal support will be enlisted at the earliest opportunity.

5.3 All evidence, in any format, will be retained securely by the Data Protection Officer, who will have sole responsibility for the authorising of access to other personnel as appropriate.

5.4 In the event of multiple 'incident' Reports the Data Protection Officer, will prioritise response according to the criticality of the data at risk, or the danger of further compromise to the data subjects. How incidents are assessed is set out in Appendix 3.

5.5 The Data Protection Officer is responsible for closing the incident after corrective measures have been implemented and proved effective.

5.6 Where a breach of the Data Protection Principles has been identified the responsible manager must progress the disciplinary action at informal procedure stage at a minimum taking into consideration the content and actions outlined in the Investigation Report of the Data Protection Officer.

5.7 The Data Protection Officer will determine within 72 hours of an incident occurring whether it needs to be reported to the Information Commissioners Office. Consideration of notification to the Information Commissioner is done in line with the

ICO guidance of reporting breaches of personal data.

5.8 Any incident reported which the Information Commissioner determines warrant further investigation will be reported to the Senior Information Risk Owner.

5.9 The Data Protection Officer will consider the rights and freedoms of data subjects when investigating breaches and make a decision on whether the individuals should be informed of the compromise of their information.

5.10 The Data Protection Officer will manage all complaints received from the Information Commissioners Office and where appropriate will issue any questions or requests to the appropriate Council officers, who will be required to provide the necessary information as instructed.

6 Follow up & Escalation of Actions

6.1 Any actions that arise from incidents will be passed onto appropriate officers for implementation. These actions must be implemented to mitigate the risk of future incidents and must be completed by the officer they have been assigned to.

6.2 The Information Governance Team will follow up completion of these actions within the timeframes set out in the investigation reports.

6.4 Failure to implement the required actions will be communicated to the Information Governance Board and to the SIRO. (Appendix 4)


Incident reported
Incident Logging and Prioritsation
Investigation
Resolution and Recovery
Follow up of Actions
Closure of Incident

7 Review & Update

7.1 This policy will be reviewed and updated annually or more frequently if necessary, to ensure that any changes to the Council's organisation structure and business practices are properly reflected in the policy.

Employee Responsible for the Incident	
Employee's Line Manager	
Service Area	
Reporting / Investigation Officer	
Date of Incident	
Time of Incident	
Date Incident was Discovered	
Time Incident was Discovered	

Step One: Incident Information

Summary of Incident

Step Two: Scoring Assessment

How many individuals does the data breach affect? Tick and identify your baseline score.

Score	Scenario
+0	Information about less than 11 individuals
+1	Information about less than 11 - 50 individuals
+1	Information about less than 51 - 100 individuals
+2	Information about 101 - 300 individuals
+2	Information about 301 - 500 individuals
+2	Information about 501 - 1,000 individuals
+3	Information about 1,001 – 5,000 individuals
+3	Information about l 5,001 – 10,000 individuals
+3	Information about 10,001 – 100,000 individuals
+3	Information about 100,001 + individuals
Baseline Score	

What Personal Data is included? Tick and adjust your score where applicable;

Personal (+1 for every type identified)	Tick (all that apply)
Name	☐
Address (home or business)	☐
Postcode	☐
NHS. No	☐
Email Address	☐
Date of Birth	☐
Employee Number	☐
Driving License [shows date of birth and first part of surname]	☐
IP Address	☐
Mother's maiden name	☐
Special Category (+2 for every type identified)	
Racial / Ethnic Origin	☐
Political Beliefs	☐
Religious Beliefs	☐
Trade Union Membership	☐
Physical or mental health	☐

Sexual life	☐
Biometrics; fingerprints	☐
Sensitive Data (+2 for every type identified)	
National Insurance Number	☐
Bank, Financial or credit card details	☐
Tax, benefit Records	☐
Adoption, employment, school, Social Services, housing records	☐
Child Protection	☐
Safeguarding Adults	☐
Pensions Records	☐
Other	☐
Score	

How Identifiable is the Data? Tick and adjust your score where applicable;

Score	Scenario
+0.5	It is extremely difficult to match the data to a particular person, but still, it could be possible under certain conditions
+1	It is possible to match the data to a particular person with access to additional data sources
+1.5	Identification is possible indirectly from the data breached with basic research needed to discover the individual's identity
+2	Identification is possible directly from the data breached with no special research needed to discover the individual's identity
Score	

Circumstances of the Breach. Tick and adjust your score where applicable;

Score	Scenario
+1	Compromised to a number of known recipients (e.g. One customers details send to another unrelated customer)
+1	Data altered and possibly used in an incorrect or illegal way but with the possibility to recover

+2	Compromised to an unknown number of unknown recipients
+2	Data altered and possibly used in an incorrect or illegal way without the possibility to recover
+3	The breach was due to an intentional action in order to harm the data controller or individuals
Score	

Total Score	

Step Three: Further information

1. Do you have a copy of the breached data? Please attach to report

2. Has the data been recovered?

3. Has the member of staff responsible for the incident received Bob's Business GDPR OR Cyber security training in the last 2 years? If yes - please provide date training was completed

4. Have any complaints been received regarding this breach? If yes please forward these to the Dataloss@cardiff.gov.uk.

It is a mandatory requirement that you provide a copy of the breached data. **If available please insert a copy of the information that has been breached as part of this Report Form**
Under no circumstance should you delay reporting an incident to the Information Governance Team. No internal investigation should be conducted. **Completed forms should be returned to dataloss@cardiff.gov.uk**

Appendix 2 Asset Loss Personal Data evaluation form

Asset Loss Personal Data Evaluation Form	
Name	
Employee Number	
Service	
Date of incident	
Asset Reference	
Type of Asset	
Please provide specific details regarding the nature and amount of personal data held on the asset	
Please detail your role and responsibilities?	
How did the incident occur?	

How were you made aware of your responsibilities in relation to using the device and confidential information?	

What training have you received in relation to the requirements of using the asset and ensuring its security prior to this incident?	
How is the training provided and does this involve any assessments to test your understanding?	
Can you confirm when you received this training?	
Any other comments	

Completed forms should be sent to dataloss@cardiff.gov.uk

Appendix 3

Data Protection Incident Management – Levels

"High" risk incidents pose a severe risk to Council information and will be classified as critical security incidents.

1. A widespread risk of compromising systems or compromising sensitive or critical data.

2. A breach of data involving the processing of personal data outside of the Council's supported network/systems.

3. Loss of Council assets which are not adequately protected.

4. Potential/Actual deliberate compromise of personal data

5. Investigation related to an Elected Member or member of Senior Management Team.

6. Repeated Medium/Low level incidents

"Medium" risk incidents pose a medium risk to Council information and as such will be classified as medium-severity security incidents.

1. Personal data put at risk, compromising of financial, safe guarding or where there is a risk to an individual

2. Breach involving the processing of personal data involving third party data processors.

3. ICO complaint regarding potential breach of personal data

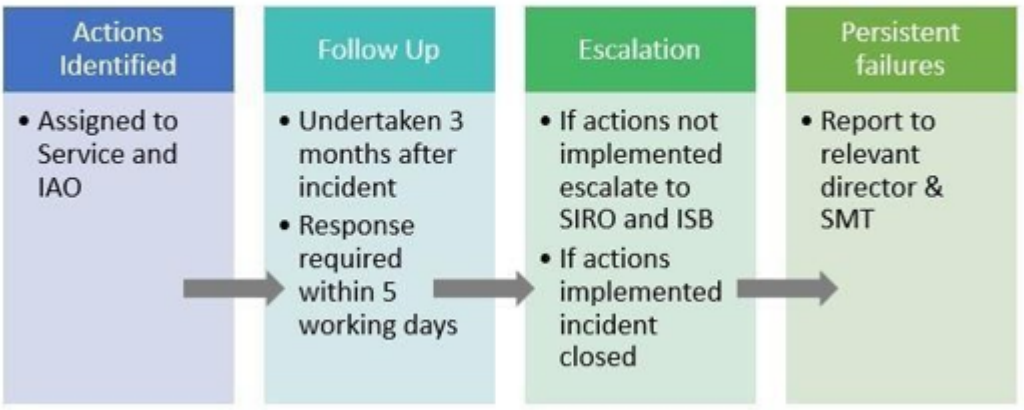
"Low" risk incidents pose a low risk to Council information and will be classified as low-severity incidents.

1. Incidents of personal data being processed incorrectly.

Including printing errors, service desk calls, internal emails and office relocations

Appendix 4

Follow up & Escalation of Actions



Appendix 5 Offences

189 Penalties for offences

(1) A person who commits an offence under section 119 or 173 or paragraph 15 of

Schedule 15 is liable—

(a) on summary conviction in England and Wales, to a fine;

(b) on summary conviction in Scotland or Northern Ireland, to a fine not exceeding level 5 on the standard scale.

(2) A person who commits an offence under section 132, 145, 170, 171 or 181 is liable—

(a) on summary conviction in England and Wales, to a fine;

(b) on summary conviction in Scotland or Northern Ireland, to a fine not exceeding the statutory maximum;

(c) on conviction on indictment, to a fine.

(3) Subsections (4) and (5) apply where a person is convicted of an offence under section 170 or 181.

(4) The court by or before which the person is convicted may order a document or other material to be forfeited, destroyed or erased if—

(a) it has been used in connection with the processing of personal data, and

(b) it appears to the court to be connected with the commission of the offence, subject to subsection (5).

(5) If a person, other than the offender, who claims to be the owner of the material, or to be otherwise interested in the material, applies to be heard by the court, the court must not make an order under subsection (4) without giving the person an opportunity to show why the order should not be made.

119 Inspection of personal data in accordance with international obligations

(1) The Commissioner may inspect personal data where the inspection is necessary in order to discharge an international obligation of the United Kingdom, subject to the restriction in subsection (2).

(2) The power under subsection (1) is exercisable only if the personal data— (a) is processed wholly or partly by automated means, or

(b) is processed otherwise than by automated means and forms part of a filing system or is intended to form part of a filing system.

(6) It is an offence—

(a) intentionally to obstruct a person exercising the power under subsection (1), or

(b) to fail without reasonable excuse to give a person exercising that power any assistance the person may reasonably require.

145 False statements made in response to an information notice

It is an offence for a person, in response to an information notice—

(a) to make a statement which the person knows to be false in a material respect, or

(b) recklessly to make a statement which is false in a material respect.

170 Unlawful obtaining etc of personal data

(1) It is an offence for a person knowingly or recklessly—

(a) to obtain or disclose personal data without the consent of the controller,

(b) to procure the disclosure of personal data to another person without the consent of the controller, or

(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

(4) It is an offence for a person to sell personal data if the person obtained the data in circumstances in which an offence under subsection (1) was committed.

(5) It is an offence for a person to offer to sell personal data if the person—

(a) has obtained the data in circumstances in which an offence under subsection (1) was committed, or;

(b) subsequently obtains the data in such circumstances.

(6) For the purposes of subsection (5), an advertisement indicating that personal data is or may be for sale is an offer to sell the data.

(7) In this section—(a) references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the GDPR or section

59(8) or 105(3) of this Act (processor to be treated as controller in certain circumstances);

(b) where there is more than one controller, such references are references to the consent of one or more of them

171 Re-identification of de-identified personal data

(1) It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.

(2) For the purposes of this section and section 172—

(a) personal data is "de-identified" if it has been processed in such a manner that it can no longer be attributed, without more, to a specific data subject;

(b) a person "re-identifies" information if the person takes steps which result in the information no longer being de-identified within the meaning of paragraph (a)

(5) It is an offence for a person knowingly or recklessly to process personal data that is information that has been re-identified where the person does so—

(a) without the consent of the controller responsible for de-identifying the personal data, and

(b) in circumstances in which the re-identification was an offence under subsection (1).

(8) In this section—

(a) references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the GDPR or section 59(8) or 105(3) of this Act (processor to be treated as controller in certain circumstances);

(b) where there is more than one controller, such references are references to the consent of one or more of them

173 Alteration etc of personal data to prevent disclosure

(1) Subsection (3) applies where—

(a) a request has been made in exercise of a data subject access right, and

(b) the person making the request would have been entitled to receive information in response to that request.

(2) In this section, "data subject access right" means a right under—

(a) Article 15 of the UK GDPR (right of access by the data subject);

(b) Article 20 of the UK GDPR (right to data portability);

(c) section 45 of this Act (law enforcement processing: right of access by the data subject);

(d) section 94 of this Act (intelligence services processing: right of access by the data subject).