THE SAINTS FEDERATION

# GDPR Policy

**Document Control**

| | |
|---|---|
| **Organisation** | The Saints Federation |
| **Title** | GDPR Policy - Data Protection Incidents Policy & Procedure |
| **Author** | Schools Information Governance Support Officer on behalf of the Data Protection Officer |
| **Owner** | Executive Headteacher 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 | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

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

Signed by the Executive 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 device.

## 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 General Data Protection Regulation
Human Rights Act (1998)
Privacy and Electronic Communications Regulations (2003)

## 3 Responsibilities

3.1 The Executive Headteacher and Governing Body, supported by 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 SchoolsInformationManagement@cardiff.gov.uk immediately, but no longer than 24 hours after which the incident was known . 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 Reporting should be via the Schools Data Protection Incident Report Form at Appendix 1 of this Policy. It should be emailed to SchoolsInformationManagement@cardiff.gov.uk

Headteachers or School staff 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 Statutory 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 school has lost control of the processing of data that 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 Schools Data Protection Policy & Procedure.

4.2 Examples of Data Protection incidents would include loss of paper-based records that contain personal/confidential information of third party individuals, including citizens, businesses, employees, children or parents; 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, or loss of an asset such as laptops, storage devices, mobile phones etc.

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 Data Protection Officer via SchoolsInformationManagement@cardiff.gov.uk

4.4 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 SchoolsInformationManagement@cardiff.gov.uk AND report it immediately to the Executive Headteacher.

**5 Management of Reported Incidents**

5.1 The Data Protection Officer, on behalf of the Executive Headteacher and Governing Body 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. All evidence will be retained for a period of seven years.

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.

5.5 The Data Protection Officer is responsible for closing the incident after corrective measures have been set out. The Data Protection Officer will require evidence of actions being implemented or rejected which will be stored as part of the investigation file.

5.6 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.

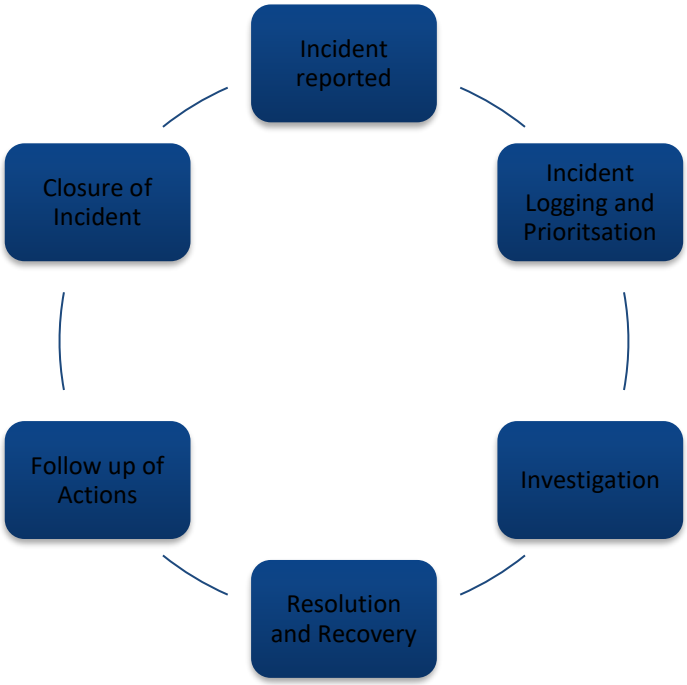
5.7 The Data Protection Officer will consider the rights and freedoms of data subjects when investigating breaches and make a decision on whether the individuals should be informed of the compromise of their information.

5.8 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 the Executive Headteacher and Governing Body for consideration .These actions must be implemented to mitigate the risk of future incidents, however the school as the data controller is ultimately responsible for determining how actions will be taken forward.

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




## 7 Review & Update

7.1 This policy will be reviewed and updated every 3 years 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.

**Appendix 1**
**Data Protection Incident Report Form**

| Schools Data Protection Incident Report Form | |
|---|---|
| **Name (person reporting)** | |
| **School** | |
| **Date & Time of Incident** | |
| **Headteacher** | |
| **How did the incident occur? Please provide specific details** | |
| **What data has been disclosed?** | |
| **Amount of personal data compromised? E.g. how many individuals have been affected?** | |
| **If available - Please insert a copy of information that has been breached** | |
| **Have you received any complaints in relation to this breach? If so please email these to SchoolsInformationManagement@cardiff.gov.uk** | |

****Under no circumstance should you delay reporting an incident to the Information Governance Team, and no internal investigation should be conducted****

**** All incidents must be reported within 24 hours****

**Completed forms should be sent to SchoolsInformationManagement@cardiff.gov.uk**

**Appendix 2**

**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 that the person knows to be false in a material respect, or
(b) recklessly to make a statement that 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 GDPR (right of access by the data subject);
(b) Article 20 of the 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).