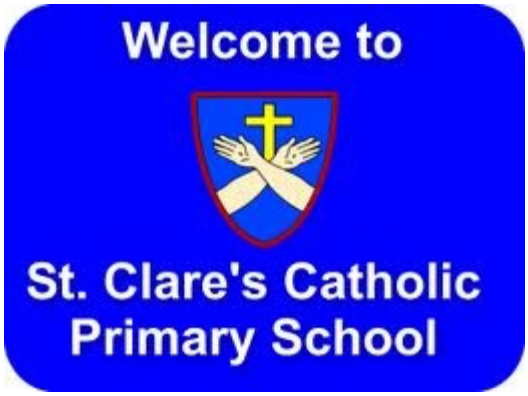

St Clare’s RC Primary School

Data Breach Management Procedure

Investigating and Reporting data breaches.

Document Control

Revision History

Version	Date	Author	Description of Change
0.01	20/04/2020	Fiona Cosgrove	Document created

1. Introduction

What is a Data Breach?

A personal data breach means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. A breach is more than just about losing personal data. It includes:
• Access by unauthorised 3rd party
• Deliberate or accidental action / inaction by the School or its contractor
• Alteration of personal data without permission (integrity breach)
• Loss of availability of personal data. (Availability breach)

How to deal with a Data Breach

All School staff have a duty to report data breaches to a Senior Manager as soon as they become aware of them. This is to ensure that incidents are controlled, investigated and resolved as quickly as possible. Under the General Data Protection Regulation ('GDPR') if there is a likelihood of a risk to people's rights and freedoms as a result of a data breach the breach must be notified to the ICO **within 72 hours of becoming aware of it**.

The School is at risk of fines of up to 20 million euros for a data breach and up to 10 million euros for a failure to comply with a requirement to report a data breach to the ICO as required.

This procedure describes the roles, responsibilities and processes required to ensure data breaches are properly handled. It provides practical advice and sources of help for all staff involved in reporting and managing information security incidents.

In brief the procedure for handling data breaches is as follows:
• All staff are responsible for **immediately** on becoming aware of an incident alerting a senior manager in their service of a data breach. This should take place by phone or face to face.
• The senior manager is responsible for carrying out an investigation, completing the incident report using the standard on line breach reporting form, allocating a severity level / assessing risk and escalating any level 1 and 2 breaches to the Senior Leadership Team (SLT) and any level 3 and 4 breaches **within 48 hours** of staff becoming aware of the breach.
• If there is a likelihood of a risk to people's rights and freedoms the breach must be notified to the ICO **within 72 hours of becoming aware of the breach**. The

responsibility for reporting the breach to the Information Commissioners Office (ICO) within 72 hours (and data subjects if appropriate) in respect of:
• The majority of breaches rests with SLT
• Breaches committed by the head rest at Governor level

The Data Protection Officer (DPO) (or a deputy) must be consulted in **all** cases prior to reporting to the ICO but the investigation is the responsibility of the Service. The 72 hour report may need to be supplemented by further report if a fuller investigation is required. This should run in parallel.

If members of SLT are likely to be unavailable (e.g. due to annual leave or other commitments) they should make suitable prior arrangements (e.g. by arranging for another appropriate staff member to undertake ICO reporting of Data Breaches on their behalf) to ensure deadlines are met and should indicate on their out of office message who their nominee is for dealing with Data Breach Reporting.

The management and investigation of incidents involving data shared with or by the School may also demand a collaborative approach with relevant data sharing partners to learn lessons, strengthen data sharing arrangements and the management and assessment of adverse impacts.

2. Key Stages

- Reporting a data breach to a Senior Manager.
- Containment of and recovery from the incident.
- Assessment and creation of report.
- Notification of the breach (where necessary) to the Information Commissioner and the individual/s whose personal data has been compromised.
- Evaluation and response.
- Learning Lessons.
- Closure

A flowchart of the process is at Appendix 1.

3. Reporting to a Senior Manager

Bearing in mind the timescales for mandatory data breach reporting, speed is of the essence when assessing and controlling an incident as most data breaches will need to be notified to the Information Commissioner's Office and in high risk cases, the individual/s whose personal data has been compromised will also need to be notified.

All incidents related to the loss/theft of ICT assets should also be reported to your ICT Service Provider, to enable immediate actions to be taken to block unapproved use of the missing device.

1. Staff *must* notify incidents to a Senior Manager immediately on becoming aware of a data breach.

It is essential staff report data breaches immediately on becoming aware of them.

4. Containment

Where data has been inappropriately disclosed to an external party steps should be taken as a priority to recover the compromised data directly from the unintended recipient to limit the impact for those affected and for the School.

The following examples indicate the circumstances where there is a likelihood of recovering compromised data or, ensuring that it is not further misused or disclosed:

- Where the 'incident reporter' is the unintended recipient.
- Letter posted or hand delivered to the wrong recipient, provided the incorrect address remains available.
- Asking the unintended recipient of the misdirected email to confirm it has been deleted.
- Ascertaining if CCTV covers the locations of papers or equipment lost or stolen in a public place (in theft cases, knowing CCTV footage exists may assist the police seeking disclosure of public or private footage).

Depending on the circumstances, where the identity and actual address of the unintended recipient is known, a formal letter or undertaking, promising not to disclose the content of any inappropriately disclosed information may be necessary, even where this is recovered. This might be appropriate in any case where it is believed the unintended recipient knows the subject(s) of the compromised information.

5. Investigation, Assessment and writing Investigation report.

The Senior Manager is responsible for carrying out an investigation, completing the incident report, using the standard data breach reporting form, and allocating a severity level/assessing the risks (see table at Appendix 3).

Severity allocation is an important part of the risk assessment but is for internal use only. Severity levels do not form part of the report to the ICO.

The Senior Manager must establish:

- What has happened,
- When it happened (date and time),
- How and why it has happened,
- How it came to light,
- Details of the people affected,

- Who was involved,
- The action necessary to contain the incident and reduce the risk of it reoccurring.

Investigation of an incident may include some or all of the following:

- Statements from key individuals or witnesses involved.
- Interviews from key individuals or witnesses involved.
- Interview with the person affected (where appropriate).
- Inspection of the location of the incident or any equipment involved.
- Examination of any physical evidence/documentation available.

Investigating Data Breaches – The Main Requirements.

The following highlights some of the issues the Senior Manager will need to consider:

- What Severity/Risk Level (See below).
- The types of data that are involved e.g. financial or **special category data**.
- Who could be harmed and in what way?
- Whether any lost or stolen data can be recovered.
- What lessons need to be learnt?

Special Category Data.

When considering the risk for the School and the individual/s whose personal data has been compromised arising out of the incident you should consider what information is personal or not and whether it constitutes one of the special categories of personal data (previously sensitive personal data) or not.

'Personal' data relates to any living individual who can be identified from data, or

The Senior Manager must carry out an investigation and complete the online data breach reporting form within 48 hours of becoming aware of the breach.

from that data. The 'special categories' of personal data includes information on:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union memberships.
- Genetic data.
- Biometric data for uniquely identifying a living individual.
- Health.
- Sexual life or sexual orientation.

- Commission or alleged commission of any offence or alleged offence and any proceedings in relation to any offence or alleged offence.

Guidance on investigation is set out at Appendix 2 below.

Where need the Senior Manager should involve colleagues in relevant services to support of contribute to investigations. Examples of relevant services include:

- For NHS or social care data in Children and Families – Information Governance Team and Caldicott Guardian.
- Compromise of ICT systems or equipment (e.g. virus attacks, network breaches) – ICT Service Provider.

The Senior Manager must always take all steps to ensure that their investigation into the incident does not prejudice any potential future legal investigation/action that may need to be carried out.

It is essential that the Senior Manager completed the data breach report including the severity level assessment with **48 hours of the School becoming aware of the data breach. Guidance on determining severity levels at Appendix 2.**

6. Notification.

The SLT member must review and quality check all ICO reports as soon as the completed report is logged to ensure they are appropriately completed.

Notifying the ICO.

The School must within 72 hours of becoming aware of the breach report to the ICO any data breach where there is a likelihood of risk to individuals' rights and freedoms. If the notification to the ICO is made after this 72 hour period it should be accompanied by reasons explaining the delay. There may be cases where the 72 hour report may need to be supplemented by further report if a fuller investigation is required. This fuller investigation should run in parallel.

Although the ICO guidance currently suggests reporting by telephone in the first instance (and states the ICO will send a copy of the information reported back) this procedure requires written reporting using the ICO form in all cases to ensure there is a proper audit trail.

All breaches reported to the Information Commissioner should be made on the Information Commissioner's standard form which can be accessed via the following link:

https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

The link also sets out the Information Commissioner's general guidance on personal data breaches.

If the data breach is unlikely to result in any risk to individuals then it doesn't have to be reported to the ICO. However, if it is decided that there is no need to report the breach, this decision needs to be able to be justified and reason must there be documented by the SLT member.

Examples given by the ICO of non-reportable breaches include loss of encrypted laptop or the loss or inappropriate alteration of a staff telephone list.

The DPO (or a deputy) must be consulted in all cases prior to reporting to the ICO but the investigation is the responsibility of the school.

The ICO will require the following information as a minimum:

- A description of the nature of the personal data breach including, where possible;
    - The categories and approximate number of individuals concerned; and
    - The categories and approximate number of personal data records concerned.
- The name and contact details of the DPO or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Notifying Individuals whose Personal Data is compromised.

Any individuals whose personal information has been lost or released where there is a high risk to the individuals must be notified ASAP. The responsibility for notifying rest with SLT.

Other People who may need to be notified.

Other people who need to be notified include:

- Data sharing partners with whom any other relevant regulatory bodies may need to be contacted but this needs to be agreed with the SLT member.
- The Court if Court documents are lost.
- Data sharing partners from whom the compromised data originated.

- Companies whose commercial interests may be adversely affected.

7. Evaluation.

One of the key purposes of the investigation is to identify the 'root causes' that led or contributed to the data breach and to try and prevent similar data breaches across the Council. Consider for example:

- If the incident has arisen from defective corporate technical controls, policies, procedures or from inadequate local controls.
- If an employee ought to have been reasonably aware of the school's expectations and the consequences of breaching corporate/local data protection/information security policies/procedures.
- What training the employee has received?

Close the incident.

- If the incident highlights further training needs (and if so, in what area)
- What recommendations should be made to address the root causes identified?
- Can you identify the risks and issues that, whilst not 'in scope' of the incident, are appropriate for separate follow-up and actions?

The DPO will consider if a similar incident has been reported previously and report to the SLT member on any systemic issues/changes that need to be made across the Council to prevent future occurrences.

8. Closure.

Where the Information Commissioner is notified, the closure of the incident must not take place until the Information Commissioner informs the Council of any further remedial action and/or enforcement measures that may be required, and these are

Evaluating lessons to be learnt.

implemented. If a decision is made not to implement the recommendation, this must be supported by an appropriate rationale which should be agreed with the relevant SLT member.

The incident should be closed only when all recommended actions have been completed to the satisfaction of the relevant DSIRO or DDSIRO. DSIROs and DDSIROs are responsible for ensuring a record of closed investigation is kept.

Appendix 1 – Flow chart

Member of staff becomes aware of Data Breach - **T1**

Immediately

Reports data breach to a Senior Manager

ASAP.

Steps taken to contain the data breach.
Within 48 hours of T1

Senior Manager investigates and fully completes reporting form (referring to Data Breach Guidance)

ASAP after 48 hours of T1

Report finalised by SLT member who notifies individuals if there is a high risk to individuals DPO consulted in all cases

Within 72 hours of T1

SLT notifies ICO

Within 1 week of T1

Assessment / lessons learnt completed.

On receipt of outcome from ICO

CASE CLOSED

Appendix 2 – Basic facts required for report completion.

Basic facts should be gathered and include:

- The name and contact details of incident report (i.e. external complainant, member of public, employee, data processor, data sharing partner) and the person responsible for the breach. **For confidentiality reasons, reports should be anonymised.**
- Date, time and location of incident.
- When did the School become aware of the breach?
- What categories of personal information are included in the breach?
- What categories of data subjects are affected?
- What happened, how it happened and who was involved.
- The nature, extent and sensitivity of the compromised information.
- Is it a cyber breach?
- Has it been contained and if so how and how quickly?
- Numbers of individuals or third parties affected.
- What the information reveals and if/how it could cause harm to those it concerns.
- Whether any of the information was supplied partly or wholly by third parties.
- What is the severity level (see Appendix 3 for guidance)?
- Whether the theft and/or loss of equipment has been reported to the Police.
- What training has the person responsible for the breach completed and when.
- What action needs to be taken to prevent a similar breach happening in the future?
- What School Policies and Guidance are relevant and was the person responsible aware of these policies/guidance.

Appendix 3 – Guidance on Determining Severity Level of Breach.

The Senior Manager must make a substantive determination of the severity level of an incident i.e. what is its potential impact on the individual/s whose personal data has been compromised. NB: **Internal use only. Severity levels do not form part of the report to the ICO.**

The table below gives guidance on Severity Levels. **However, each case must be considered on its facts.**

Severity	Impact	Interpretation
Level 0	No loss of control* of personal or sensitive information.	
Level 1 (Low Risk)	Loss of control* of **one or more** individual's personal data but the severity and impact on the individual is minimal e.g. has been quickly contained/recovered.	
Level 2 (Medium Risk)	Loss of control* of **one or more** individual's personal data and there is a risk of impact to the individual(s).	
Level 3 (High Risk)	Loss of control* of **one of more** individual's personal data and there are serious potential consequences on the individual(s).	
Level 4 (Very High Risk)	Loss of control* of **a significant number** of individual's personal data which falls within one of more of the special categories of data and is likely to cause harm to those individuals as well as to lead reputational damage to the School.	

Loss of control includes:

- Access by unauthorised 3rd party.
- Deliberate or accidental action/inaction by the School or its contractor.
- Alteration of personal data without permission (integrity breach)
- Loss of availability of personal data. (availability breach)

In determining severity the following will be relevant:

- The type of breach
- The nature, sensitivity and volume of personal data
- The ease of identification of individuals
- The severity of consequences for individuals
- The special characteristics of the individual
- The number of individuals affected
- The special characteristics of the data controller

Does the data breach:

- Pose a threat to human life or safety?
- Cause distress or substantial distress to the privacy or well-being of one or many individual(s)?
- Compromise the School's ability to meet its regulatory, statutory or contractual obligations?
- Pose a threat to business continuity in the School?
- Prejudice an investigation or facilitate the commission of crime?
- Damage the commercial interests or, reputation of a third party organisation?

What type of data is involved?

- Is it one of the special categories of personal data?
- Is it sensitive because of its very personal nature (e.g. Health, Social Care, Children's records) and/or because of what might happen if it is misused (bank accounts details, risk to physical safety)?

If the data has been lost or stolen, is there protection in place, such as encryption?

What does the data tell a third party about the individual? Is it only one details about them, such as a telephone number, or does it include other private details that could help a fraudster build a detailed picture? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?

Is the breach internal to the organisation, no public release occurred, or the data in question was quickly retrieved or deleted?

Have any individual(s) suffered actual harm?