Data Breach Notification Procedure for Schools

Version 1 - March 2018
Owner: Brent Council Data Protection Officer on behalf of

Saint Joseph's Infant and Junior Schools

Review Date: March 2019

Scope

This procedure applies in the event of a personal data breach. This conforms to the GDPR Article 33 “Notification of a personal data breach to the supervisory authority” and the GDPR article 34 “Communication of a personal data breach to the data subject”. The GDPR draws a distinction between a ‘Data Controller’ and a ‘Data Processor’ in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Each organisation should establish whether it is a data controller, or a data processor for the same data processing activity; or whether it is a joint controller. This procedure is primarily concerned where Amanda Whelan is a Data Controller or a Joint Data Controller.

Definitions

Personal data
“means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”. For schools, this is likely to include employees, pupils, parents, guardians and governors.

Personal data breach
“a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.”

Data Controller
“means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data”. In most cases this will be the School.

Data Processor
“means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”

Supervisory Authority
“means an independent public authority which is established by a Member State.” The Information Commissioner’s Office (ICO) is the Supervisory Authority for the UK.

Responsibility

All employees (permanent and temporary staff), contractors, governors, and business partners are required to be aware of, and to follow this procedure in the event of a personal data breach.
All employees, contractors, governors, and business partners are responsible for reporting any personal data breach to the Data Protection Officer as soon as they become aware.

Procedure – Breach Notification to Data Protection Officer

All employees should report all data breaches to the Data Protection Officer and to your internal school contact.

Brent Council Data Protection Service	Internal school contact
Data Protection Officer	Amanda Whelan Executive Head teacher
020 8937 2018	02089036032
school.dpo@brent.gov.uk	admin@sjinf.brent.sch.uk

DBF1 – Data Breach Reporting Form should be completed when reporting a data breach and a copy should be sent to the Data Protection Officer school.dpo@brent.gov.uk to investigate and to make final recommendations.

Please note that there is a 72 hours notification deadline to report qualifying breaches to the ICO and this starts from the time either your School or your Data Processor / Service Provider first becomes aware of a breach incident or potential incident.

Procedure – Breach Notification of Data Processor to Data Controller

In arrangements whereby Amanda Whelan is a Data Processor then Amanda Whelan reports any personal data breach or security incident to the Data Controller without undue delay. These contact details are recorded in the Internal Breach Register.
Amanda Whelan provides the controller with all of the details of the breach.
The breach notification is made by two forms of communication, by email and by a phone call. A confirmation of receipt of this information is made by email.

Procedure – Breach Notification of Data Controller to Supervisory Authority (ICO)

Amanda Whelan and your Designated Data Protection Officer will determine if the supervisory authority need to be notified in the event of a breach.
Amanda Whelan assess whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, by conducting a data protection impact assessment against the breach.

If a risk to data subject(s) is likely, Amanda Whelan Data Protection Officer reports the personal data breach to the supervisory authority [ICO] without undue delay, and not later than 72 hours. This shall be done in two forms of communication (email and phone call).
If the data breach notification to the supervisory authority [ICO] is not made within 72 hours, Amanda Whelan Data Protection Officer submits it electronically with a justification for the delay.

If it is not possible to provide all of the necessary information at the same time Amanda Whelan will provide the information in phases without undue further delay.
The following information needs to be provided to the ICO:

- A description of the nature of the breach.
- The categories of personal data affected.
- Approximate number of data subjects affected.
- Approximate number of personal data records affected.
- Name and contact details of the Data Protection Officer.
- Consequences of the breach. This includes those that have already occurred and those that are likely to occur.
- Any measures taken to address the breach.
- Any information relating to the data breach. This may be submitted in phases.

The Data Protection Officer notifies the ICO. Contact details for the supervisory authority are found at www.ico.org.uk.

In the event the ICO assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.

The breach notification is made by email and phone call.

A confirmation of receipt of this information is made by email and phone call.

Procedure – Breach Notification of Data Controller to Data Subject

If the personal data breach is likely to result in high risk to the rights and freedom of the data subject(s), Amanda Whelan notifies the data subject(s) affected immediately in accordance with the Data Protection Officer's instructions.
The notification to the data subject(s) describes the breach in clear and plain language and includes the following information:

- A description of the nature of the breach.
- The categories of personal data affected.
- Approximate number of data subjects affected.
- Approximate number of personal data records affected.
- Name and contact details of the Data Protection Officer.
- Consequences of the breach. This includes those that have already occurred and those that are likely to occur.

- Any measures taken to address the breach.
- Any additional information relating to the data breach.

Amanda Whelan takes measures to render the personal data unusable to any person who is not authorised to access it using encryption.
The data controller takes subsequent measures to ensure that any risks to the rights and freedom of the data subject(s) are no longer likely to occur by recording and tracking remedial actions.
If the breach affects a high volume of data subjects and personal data records, Amanda Whelan makes a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder Amanda Whelan's ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner.
If Amanda Whelan has not notified the data subject(s), and the ICO considers the likelihood of a data breach will result in high risk, Amanda Whelan will communicate the data breach to the data subject(s) by following the instructions issued by the ICO.
Amanda Whelan documents any personal data breach(es), incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.
Amanda Whelan shall discuss data breach(es) at the Senior Management Team meetings (SMT).
Amanda Whelan's Data Protection Officer shall prepare a quarterly report on Information Security for SMT.

Document Control

The Data Protection Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the requirements of the GDPR and UK Data Protection legislation.