[Insert own logo]

GDPR DATA PROTECTION

Personal Data Breach Procedure

The Three Saints Academy Trust

Data breach procedure

Document version control

Version	Author	Date	Approved by	Effective from
1.0 draft	Jo Kaptijn	1/5/2018		
2.0	Three Saints	15/5/2018	Directors	15/5/2018

Key contact details

The Three Saints Academy Trust

Data Protection Officer – Ton Kaptjin
Data Protection Lead – Kim Sawe

IT Service Desk – Neil Gilhooley

Contents

Introduction

This policy applies in the event of a personal data breach under Article 33 Notification of a personal data breach to the supervisory authority, and Article 34 Communication of a personal data breach to the data subject of the General Data Protection Regulation (GDPR).

Simply put, the procedure applies to all data breaches including computer security incidents as defined and explained below.

Why?

The GDPR introduced a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (The ICO). This must be done within 72 hours of becoming aware of the breach, where feasible.

- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, individuals must be informed without undue delay.
- Organisations should ensure they have robust breach detection, investigation and internal reporting procedures in place. This will facilitate the decision to notify the ICO and the affected individuals or not.
- Organisations must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Who

This procedure applies to **all staff and managers** (whether employees, contractors or temporary staff) of The Three Saints Academy Trust.

- Everyone is required to be aware of, and to follow this procedure in the event of a personal data breach;
- The Organisation's Data Protection Officer (DPO)/Data Protection Lead and other managers/IT service desk as appropriate - have responsibilities to contain/restore the data breach and assess the risks to individuals;
- The Data Protection Officer - will notify the ICO of the breach within 72 hours and inform all Data Subjects that have been compromised in any Data Breach where required to do so;

- Head teachers – will ensure training is provided to ensure all staff are aware of this procedure and how to find/implement it.

Definitions

The Organisation – The Three Saints Academy Trust is the establishment acting as a Data Controller which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Personal data - Any information relating to an identified or identifiable living person ('data subject') i.e. someone who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to information regarding the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Data breach - The accidental or unlawful loss, destruction, alteration or unauthorised disclosure of personal data that can occur for many reasons, IT failures through to human error. They can fall into one or more of these categories:

- **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, personal data;
- **Integrity breach** - where there is an unauthorised or accidental alteration of personal data;
- **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

Examples of data breaches

- Loss or theft of paper records or loss or theft of equipment on which data is stored e.g. laptop, mobile phone, tablet device, memory stick;
- Letter or email containing personal and/or confidential data sent to the wrong address or an email to unauthorised group email boxes;
- Personal data disclosed orally in error in a meeting or over the phone – including 'blagging' where information is obtained by deceiving The Trust, or where information has been disclosed without confirming the true identity of the requester;

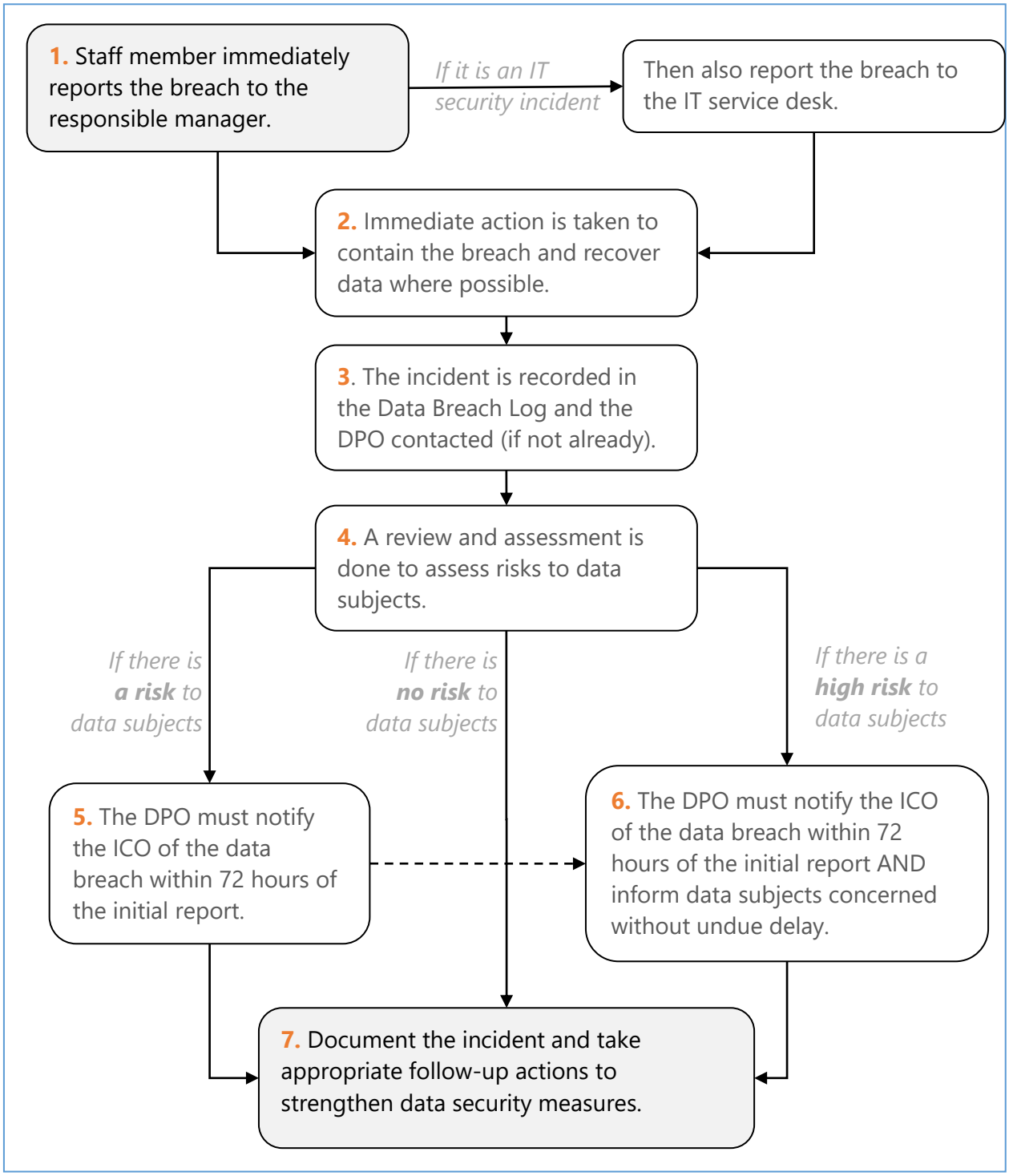
- Unauthorised access to information classified as personal or confidential e.g. attaching documents to an outlook diary appointment that is openly accessible;
- Posting information on the world wide web or on a computer otherwise accessible from the Internet without proper information security precautions;
- Sensitive information left on the photo-copier or on a desk in a public area;
- Unauthorised alteration or deletion of information;
- Not storing personal and confidential information securely;
- Not ensuring the proper transfer or destruction of files after closure of offices/buildings e.g. not following building decommissioning procedures;
- Failure to safeguard/remove personal data on office equipment (including computers and smart phones) before disposal/sale.

Example data breaches caused by IT Security Incidents

- Unauthorised access to the IT systems because of misconfigured and/or inappropriate access controls;
- Hacking or phishing attack and related suspicious activity;
- Virus or malware attacks and related suspicious activity;
- ICT infrastructure-generated suspicious activity;
- Divulging a password to another user without authority.

Procedure overview

When a member of staff detects or suspects a potential personal data breach …



Personal data breach procedure

Procedure steps

1. Reporting the data breach

Anyone who detects or suspects a personal data breach or an IT security incident, must report it immediately!

- ***Report to*** the Headteacher
- If the breach is related to an IT security incident, the Headteacher will ***report to IT Lead***

Why?

Timeliness of reporting is key to ensure we can put measures in place to contain the damage and recover the data if possible and to assess how severe the breach is for the people whose data has been compromised.

2. Contain the breach and recover data

The Headteacher must take immediate action to contain the breach and to recover any information disclosed or lost.

Why?

To reduce the impact on individuals whose personal information is/could be at risk (for example, ensuring any emails sent to the wrong people have been deleted).

3. Record the incident in the Data Breach Log

Once any immediate damage is contained, the Headteacher needs to record a detailed description of the breach in the Data Breach Log and inform the DPO & Trust CEO if they are not already involved.

The type of information that should be recorded initially (and after the incident review and risk assessment) includes:

- A description of the nature of the breach;
- Number of data subjects and personal data records affected;

- The categories of personal/sensitive data affected;
- Likely consequences of the breach;
- Any measures that have been or will be taken to address/mitigate the breach.

This step needs to be done straight away.

Why?

- To give the Trust/DPO time to assess the severity of the breach, who needs to be informed and to investigate how it occurred/what actions are needed to remove any vulnerabilities.

4. Incident review and risk assessment

The GDPR gives the following explanation of possible risks and consequences related to a data breach:

"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."

The risk assessment (RA) must be carried out straight away to establish what personal/sensitive data was involved in the breach and to determine the likelihood and severity of the resulting risk to those concerned. It should also outline what data protection precautions have been taken and any further actions needed.

Why?

- To establish if there is a risk to data subjects so that they and/or the ICO are informed.
- To understand how the breach occurred and use lessons learnt to improve school systems, policies and procedures.

4.1 Criteria for notification and justification

The output of the risk assessment will decide the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

- If there is **no risk** to data subjects e.g. the incident involves encrypted data for which there is another existing source, then the DPO doesn't have to notify the ICO or data subjects but needs to justify this decision in the documentation;
- If there **is a risk** to data subjects, the DPO must notify the ICO as soon as possible and within 72 hours;
- If there a **high risk*** to data subjects, then those concerned must also be informed directly and without undue delay.

  * If the impact of the breach is assessed as more severe, the risk is higher; if the likelihood of the consequences is greater, then the risk is higher.

5. Notifying the ICO

The DPO must notify the ICO within 72 hours of the breach and provide the following information (if it is not all available, the ICO should be notified and advised when any additional information will be provided).

Notification is made by email, phone call.

Confirmation of receipt of this information is made by email, phone call**.**

Information sent to the ICO is a description 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 data protection officer (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.

Why?
It's the law. If the breach is not reported, the school could be liable to a fine or other enforcement action.

6. Notifying the data subjects

The DPO will promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them as follows:

- The breach must be described in clear and plain language, the nature of the personal data breach and similar information as supplied to the ICO, and as a minimum:
    - the name and contact details of your data protection officer 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 and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Why?

One of the main reasons for informing individuals without undue delay is to help them take steps to protect themselves from the effects of the breach.

7. Appropriate actions and documentation

The DPO/Organisation must complete its document on the incident and monitor/document the appropriate follow-up actions taken to strengthen data security measures.

Why?

- This type of record keeping is key to the school demonstrating 'accountability' for data protection in line with the GDPR legislation.