St George's CE Primary School

GDPR Breach Management and Response

Policy and Procedure

Version 1.0

May 2018

Contents

Introduction

St George's CE Primary School collects, processes and stores personal data on pupils, parents, staff, governors, and volunteers. Under the General Data Protection Regulation, the school is a data controller of this data. If the school becomes aware of a data breach we have an obligation to respond in a manner that is compliant with the GDPR.

This document defines our obligations and how we will respond in the event of a breach. Specifically, it addresses:

- What our obligations are under GDPR
- How to assess the nature and risk from a data breach
- Procedure for responding to data breaches

What our obligations are under GDPR

Where we become aware of a breach we will:

1. Assess whether the breach results in:

    - **No risk** to the rights in which case we do not need to notify the ICO or the data subject, e.g. an encrypted memory stick is lost, and the password has remained safe.

    - A **risk** to the rights and freedoms of the individuals, in which case we must notify the ICO within 72 hours, e.g. a spreadsheet of staff names and addresses is mistakenly sent by email to another school in the area. We should contact the headteacher of the school, who should confirm that they have deleted the email without reading it.

    - A **high risk** to the rights and freedoms of the individuals, in which case we must notify the ICO within 72 hours and the data subject without delay, e.g. a computer virus results in student data being accessible to hackers.

2. Communicate the breach to the ICO and where necessary the data subject.

3. Maintain a record of the breach. This includes breaches that do not require notification

Assessing the nature and risk from a data breach

The GDPR defines a breach in Article 4(12) as:

'personal data breach' means 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

Breaches are categorised as:

(i) Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, personal data

(ii) Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, personal data; and

(iii) Integrity breach - where there is an unauthorised or accidental alteration of personal data

When assessing if a breach has a high impact we will consider:

- The category of data that is breached, i.e. are special categories of data included in the breach such as health records of students?
- The number of records breached, although even one record could result in a high-risk situation for the individual;
- The category of individual impacted by the breach, where children or vulnerable people are involved the risk is considered higher;
- The potential negative impact on the individual. High risk impacts include:
    - Identity theft
    - Fraud
    - Physical harm
    - Psychological distress
    - Humiliation
    - Damage to reputation;
- When in doubt as to the risk level we will notify the ICO and seek advice on the need to notify the individuals impacted.

Procedure for responding to data breaches

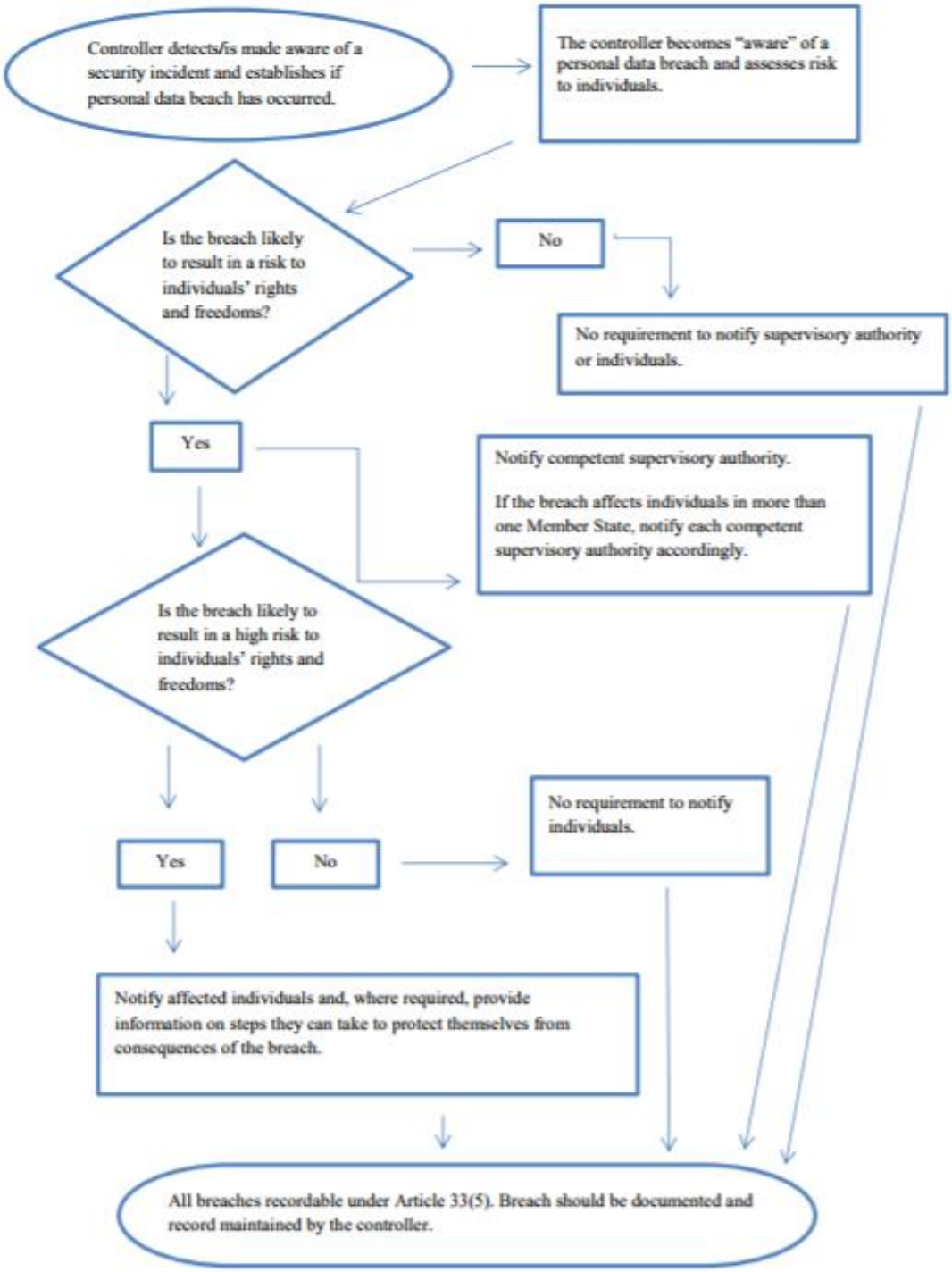
As part of our staff data protection training we make staff aware of what constitutes a data breach and of the need to inform the DPO/Headteacher in the event of a suspected breach.

In the event of a staff member becoming aware of a suspected data protection breach:

1. The staff member will inform the DPO/Headteacher;
2. The DPO/Headteacher will gather the relevant staff members to assess what has happened and the risk from the breach;
3. The DPO/Headteacher will document the breach (see appendix 1)
    a. Where necessary the DPO/Headteacher will notify the ICO as soon as possible (and not more than 72 hours from when the staff member became aware of the breach). The ICO has its contact information on the ICO website: phone 0303 123 1113.

    Where it is not possible to notify the ICO of all information immediately we will notify the ICO in phases as quickly as possible.

4. We will discuss the breach with the ICO and decide if we need to inform the data subjects;
5. Where necessary we will notify the data subjects (see appendix 2);
6. We will record the breach and keep a copy of this record.


Controller detects/is made aware of a security incident and establishes if personal data beach has occurred.
The controller becomes "aware" of a personal data breach and assesses risk to individuals.
Is the breach likely to result in a risk to individuals' rights and freedoms?
No
No requirement to notify supervisory authority or individuals.
Yes
Notify competent supervisory authority.
If the breach affects individuals in more than one Member State, notify each competent supervisory authority accordingly.
Is the breach likely to result in a high risk to individuals' rights and freedoms?
Yes
No
No requirement to notify individuals.
Notify affected individuals and, where required, provide information on steps they can take to protect themselves from consequences of the breach.
All breaches recordable under Article 33(5). Breach should be documented and record maintained by the controller.

Appendix 1: Notification of Breach to the ICO

In preparation for notifying the ICO we will document:

- What is the nature of the breach / what happened
    - Categories of data subject
    - Category of data
    - Type of breach
    - Number of records breached (to the best of our knowledge);
- The name and contact details of our DPO;
- The likely negative consequences of the data breach on the individuals impacted;
- Measures that will be taken by the school to mitigate the risk associated with the data breach. This will include immediate mitigating risks and longer-term plans to avoid a repeat of the breach.

We will communicate this information to the ICO. Where it needs to be communicated in phases we will not unduly delay the first notification

Appendix 2: Notification of Breach to the data subject(s)

In preparing for notifying the data subjects we will document:

- Some information on the breach that provides the individual with some detail and context;
- The name and contact details of our DPO;
- The likely negative consequences of the data breach on the individuals impacted;
- Measures that will be taken by the school to mitigate the risk associated with the data breach. This will include immediate mitigating risks and longer-term plans to avoid a repeat of the breach;
- Any advice that we can provide on what the individual can do to further reduce the risk to them.

MaryAnn Davison
GDPR for Schools
May 2018