WOODLANDS PRIMARY SCHOOL

DATA BREACH PROCEDURE

Updated: January 2022

Review Date: January 2023

Data Protection - Data Breach Procedure & Policy

Policy Statement

Woodlands Primary School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held Woodlands Primary School and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Woodlands Primary School if a data protection breach takes place.

1.0 Legal Context

Woodlands Primary School will comply with the requirements of Article 33 of the General Data Protection Regulations in relation to the Notification of a personal data breach to the supervisory authority

1.1. In the case of a personal data breach, the controller (the school) shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

1.2. The processor shall notify the controller (the school) without undue delay after becoming aware of a personal data breach.

1.3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

1.4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

1.5. The controller of Woodlands Primary School shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

2.0 Types of Breach

2.1. Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

3.0 Managing a Data Breach

In the event that Woodlands Primary School identifies or is notified of a personal data breach, the following steps should followed:

3.1 The person who discovers/receives a report of a breach must inform the Headteacher, the schools Data Protection Lead or the School's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable. This should be done by completing the attached breach notification form.

3.2. The DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3.3. The DPO (or nominated representative) must inform the Head/Chair of Governors as soon as possible if the breach is considered of a serious nature. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

3.4. The DPO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support should be obtained.

3.5 The DPO will take the decision based on the severity of a breach and the likely effect on data subjects as to whether the ICO should be notified (this should occur within 72 hours of the incident being identified) and to whether the data subject should be notified.

3.5. The DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. Contacting the relevant Council Department, so that they are prepared for any potentially inappropriate enquiries for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Head Teacher/DPO (or nominated representative).

c. The use of back-ups to restore lost/damaged/stolen data.

e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

f. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.