SEVENOAKS DAY NURSERY

Data Breach Procedure

Sevenoaks Day Nursery (SDN) holds personal and sensitive/special category personal data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost, shared, altered, or accessed 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 / special category personal data held by SDN.

All Nursery staff, Trustees, volunteers, and contractors, referred to herein after as 'staff', are each responsible for ensuring the data we hold is protected and reporting any, and all, data incidents appropriately. This procedure applies to all staff.

Purpose

This breach procedure sets out the course of action to be followed by all staff at SDN if a data protection breach takes place or is suspected to have taken place.

Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller 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.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

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.

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.

5. The controller 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.

Types of Breach

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.

Managing a Data Breach

In the event that the Nursery identifies or is notified of a personal data breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach, or suspected breach, must inform the Nursery Finance & HR Manager. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.
2. The Nursery Manager (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. The Nursery Manager (or nominated representative) must inform the Chair of Trustees as soon as possible. As a registered Data Controller, it is the nursery's responsibility to take the appropriate action and conduct any investigation.
4. In consultation with the Chair of the Trustees, the Nursery Manager (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where the breach may endanger a child attending the nursery, 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 Nursery's legal support should be obtained.

5. The Nursery Manager (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 County Council Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all nursery 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 Nursery Manager (or nominated representative).

   c. Contacting the County Council's Communications Division if part of the crisis service, so that they can be prepared to handle any press enquiries. The Council's Senior Communications Officer can be contacted by telephone on (01629) 538234.

   d. 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.

Investigation

In most cases, the next stage would be for the Nursery Manager (or nominated representative) to fully investigate the breach. The Nursery Manager (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner’s Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. The Nursery Manager (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach as soon as practical during the investigation.

In the case of breaches which would result in a risk to the rights and freedoms of natural persons, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach.

Every incident should be considered on a case-by-case basis. If a decision is made not to report a breach to a Supervisory Authority, the basis for this decision must be recorded as part of the investigation.

In certain circumstances, it may be necessary to contact the data subjects directly. When notifying these individuals who are affected, suspected to be affected, or at risk of being affected by the breach, the Nursery Managed (or nominated representative) should:

- Give specific and clear details, as much as is known, on what has happened and how it affects, or may affect, the individual and their data;
- Outline what the Nursery has already done, and intends to do, to help them and to minimise the impact of the breach;
- Give specific and clear advice on what they can do to protect themselves;
- Give them the opportunity to make a formal complaint if they wish (see the Nursery's Complaints Procedure);
- Inform the individual as to whether the breach has been reported to the Information Commissioner's Office and provide the necessary contact details so that the individual may make a complaint to the Supervisory Authority directly.

Review and Evaluation

Once the initial aftermath of the breach is over, the Nursery Manager (or nominated representative) should provide the investigation report to the Trustees for review. The Trustees or their nominated representative will lead on a review of the breach process to identify any learning outcomes.

If systemic or ongoing problems are identified, then an action plan must be drawn up to put address the issues.

If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance.

This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance, or on a biennial basis.

Implementation

The Nursery Manager should ensure that staff are aware of the Nursery's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the Nursery's

Data Protection policy and associated procedures, they should discuss this with their line manager or the Nursery Manager.

This procedure was adopted by the Trustees of Sevenoaks Day Nursery CIO on 15th May 2024.

Susan Dreksler
Chair