Data Breach Management Policy

Policy statement

At Little Elms we recognise that we hold sensitive/confidential information about children and their families and the staff we employ. This information is used to meet the need of the business including compliance with Ofsted, other external bodies and for daily business operation purposes.

We take our duty to ensure compliance with GDPR seriously and therefore, have adopted processes and practices across the nursery group to ensure we are able to remain compliant, handle any breaches swiftly and effectively and apply any learnings to future practice.

What is a data security breach?

A data security breach occurs if there is breach of security that leads to:

- the accidental or unlawful destruction, loss or alteration of personal data; or
- any unauthorised disclosure of or access to personal data.

Personal data includes any information about a customer, colleague, a member of the public or any other individual, including, but not limited to, name, contact details, account details and personnel records.

Examples of data security breaches include:

- Loss or theft of personal data or equipment on which personal data is stored (including mobile phones and laptops);
- Inappropriate access controls allowing unauthorised use;
- Equipment or technical failure leading to unavailability or loss of or corruption of personal data;
- Human error, for example sending an email to an incorrect recipient or forgetting to use the 'BCC' field instead of the 'CC' field;
- Hacking attack; or
- "Blagging" offences where personal data is obtained by deceiving the organisation who holds it into believing the person requesting the information is entitled to access the personal data.

A personal data breach can have serious consequences for the individuals concerned, such as identity theft and fraud and it is important that everyone takes responsibility for any potential, suspected, threatened or actual security breaches.

What do you do if there is a data security breach?

You must report immediately any potential, suspected, threatened or actual security breach to the Data Controller. The Data Controller within Little Elms is Mark Symonds (Data Controller). The Data Controller will ascertain the nature and severity of the breach and will manage the breach in accordance with this policy. The notification should be made as follows:

- Completion of Incident Form to the Data Controller (email: mark.symonds@littleelmsdaycare.co.uk)
- If receipt of the e-mail has not been confirmed within 24 hours, e-mail to the HR Manager (email: hr@littleelmsdaycare.co.uk).

The information included within the Incident For should include the following details:

- Your name, job title, telephone and email contact details;
- Description of what has happened;
- Volume of personal data involved and number of individuals affected;
- Type(s) of data involved, including personal data and which individuals this affects;

- Status of security breach: (i) potential (ii) suspected (iii) threatened (iv) actual (and if actual, has this been isolated (and how) or is it ongoing?);
- Whether the data security breach relates to a supplier arrangement and, if so, from where the security breach has originated (i.e. from us or the supplier);
- Who is aware of the breach;
- What actions have been taken to address the breach and have these mitigated any adverse effects;
- Any impacts caused as a result of the breach; and
- Any other relevant information.

Breach Management Procedures

The Data Controller, Mark Symonds, will be responsible for co-ordinating the response to data security breaches with the support of the Little Elms Heads of Departments.

Those investigating will:

- Investigate the reported breach to establish the scale and nature of the breach and the potential consequences of the breach;
- Consider what can be done to recover the loss of personal data;
- Identify the safeguards in place, or to be put in place, to protect the misuse of the personal data;
- Identify any relevant departments to assist and if appropriate, any third parties, such as banks, websites, insurers, police or credit card companies to prevent fraudulent use of personal data;
- If the data security breach relates to a supplier agreement, liaise with the relevant supplier in accordance with the terms of the relevant agreement;
- By establishing the cause, determine whether any further actions can be taken to contain the breach e.g. taking systems offline, changing access codes, finding lost equipment etc.;
- Determine the value of the personal data to the third party in receipt; and
- Take all necessary steps to mitigate the effects of the personal data breach.

The Data Controller will act as a contact point for the business and the affected individuals, and will lead the co-ordination of remedial action.

Breach Reporting

In some circumstances it will be necessary to report data security breaches involving personal data to regulators, including but not limited to, the Information Commissioner. If a breach needs to be reported to the Information Commissioner, the report must be made within 72 hours of Little Elms becoming aware of the breach. It may also be necessary to notify individuals of a data security breach if the personal data is particularly sensitive or if individuals need to take steps to protect themselves against potential misuse of their personal data.

The Data Controller shall be responsible for determining whether a data security breach needs to be reported to regulators, including but not limited to, the Information Commissioner and whether affected individuals need to be notified.

In order to evaluate whether a data security breach needs to be reported to the Information Commissioner or whether individuals need to be notified of the breach, the Data Controller shall take account of all relevant regulatory guidance and shall evaluate the likely risk to individuals. The Data Controller should consider factors including the number of individuals affected, whether special personal data was affected and the volume of personal data affected. Additionally, when carrying out this evaluation the Data Controller shall consider whether there are any risks of:

- Identity theft or fraud;
- Financial loss;
- Damage to reputation;
- Loss of confidentiality protected by professional secrecy; or

- Any significant economic or social disadvantage to the individual(s) concerned.

If a data security breach involves personal data that is being processed by us on behalf of a third party, details of the data security breach may need to be notified to that third party. The Data Controller shall be responsible for determining which data security breaches need to be notified to third parties.

Where we conclude that a data security breach needs to be reported to the Information Commissioner, the notification shall be made within 72 hours and shall include the following:

- A description of the nature of the data security breach including the categories and approximate number of data subjects and personal data records concerned;
- Details including the name and contact details of the point of contact where more information can be collected;
- A description of the likely consequences of the data security breach; and
- A description of the steps taken or proposed to be taken to address the data security breach and to mitigate any potential risks.

If we conclude that it is necessary to communicate the data security breach to the affected individuals, we will contact the individuals as soon as practicable. The notification will include the information noted above and provide individuals with advice on the steps that they can take to protect their position (if applicable).

Post breach review

Following a data security breach, the Senior Management Team shall evaluate the data security breach and shall prepare an Incident Follow UP Form for the Data Controller which shall:

- Summarise the data security breach event;
- Outline the steps taken in accordance with this policy;
- Describe the effects of the data security breach;
- Detail the measures taken by the business to prevent similar breaches happening again; and
- Set out recommendations for any additional preventative steps that can be taken, including measures to improve the breach management response.

The Data Controller shall consider the content of the post breach report and shall determine what (if any) additional steps should be taken.

Data security breach log

The Data Controller shall record details of all reported data security breaches in a data security breach log. The log must include details of the nature of the data security breach, an assessment of the severity of the breach and the potential impact on individuals, whether the breach has been reported to the regulators (and if not, the reasons why it is not necessary to report to the regulators) and the current status of the breach.

Associated Documents:

- Data Retention Policy
- CCTV Policy
- Data Protection Impact Assessment Template (Senior Management Only)
- GDPR Central Record (Held by the Data Controller)
- Confidentiality Policy
- Methods of Sharing Personal Data Policy