**Data Protection Breach Reporting Procedure**

**Bewbush Community Nursery**

**May 2019**

## 1. INTRODUCTION

1.1 Background

1.1.1 The General Data Protection Regulations places a legal requirement on Bewbush Community Nursery to provides assurance that adequate and appropriate procedures are in place for the handling of and response to security incidents involving Personally Identifiable Information.

1.2 Purpose

1.2.1 The purpose of an incident response is to ensure that:

* Data breach events are detected, reported, categorised and monitored consistently.
* Incidents are assessed and responded to appropriately.
* Action is taken to reduce the impact of disclosure.
* Mitigation improvements are put in place to prevent recurrence.
* Serious breaches can be reported to the Information Commissioner.
* Lessons learnt are communicated to the organisation as appropriate and can work to prevent future incidents.

1.3 Scope

1.3.1 This procedure applies to all staff, Contractors and representatives who process personal data for which Bewbush Community Nursery is either the Data Controller or a Data Processor.

1.4 Terminology

1.4.1 For the avoidance of doubt, the following words have the specific meanings ascribed below when used in this document:

* ‘Shall’ or ‘Must’ denote a mandatory requirement. Deviation from these shall constitute non-conformance
* ‘Shall Not’ or ‘Must Not’ denotes something that is prohibited
* ‘Should’ denotes a recommendation that is non-mandatory
* ‘Should Not’ denotes something that is not recommended
* ‘May’ denotes something that is optional.

## 2. INCIDENT MANAGEMENT

2.1 Definition

2.1.1 A Data Protection breach means a breach of security leading to the:

* Accidental
* Unlawful destruction
* Loss
* Alteration
* Unauthorised disclosure of
* Or access to personal data transmitted, stored, or otherwise processed.

2.1.2. This can be as the result of an event or series of events where Personally Identifiable Information (PII) is exposed to unauthorised or inappropriate processing that results in its security being compromised. The extent of damage or potential damage caused will be determined by the volume, sensitivity and exposure of the PII.

2.1.3 Breach management is focused on detecting, reporting and containing incidents with the intention of implementing further controls to prevent the recurrence of the event.

2.1.4 Examples of common incidents are:

* Technical data corruption
* Malware
* Corrupt code
* Hacking
* Physical unescorted visitors in secure areas
* Break-ins to sites
* Thefts from secure sites
* Theft from unsecured vehicles/premises
* Loss in transit/post
* Human Resources data input errors
* Non-secure disposal of hardware or paperwork
* Unauthorised disclosures
* Inappropriate sharing

2.1.5 The proforma at Annex A is to be used for the reporting of ALL suspected data protection breaches.

2.2 Management Statement of Intent

2.2.1 Bewbush Community Nursery shall:

* Put measures in place to ensure that awareness of data protection will enable breaches to be reported more easily
* Issue guidance on how to report PII breaches for analysis, categorisation and response
* Provide resource to analyse reported PII breaches to identify those that are incidents requiring a structured response
* Ensure that its contemporaneous logs of incidents are kept
* Hold periodic post resolution lessons learned meetings to focus on trends and improvements to reduce the likelihood and impact of recurrence, as appropriate.

2.2.2 Bewbush Community Nursery recognises that in some instances PII breaches are beyond its reasonable control and the importance of being prepared for such eventualities.

2.2.3 Bewbush Community Nursery shall ensure that it reacts appropriately to any actual or suspected PII breaches occurring either within the company and its systems or with data processors.

### 2.3 Outline Process for Incidents

2.3.1 Diagram below shows the flow of actions involved in a PII Breach

Investigation

2.3.2 Discover/Identify/Assess/Investigate - Breaches and weaknesses need to be reported at the earliest possible stage to the [nominated senior person/ role] or in his/ her absence, the designated senior manager, in the form of Annex A. Only in urgent circumstances, can incidents be reported in other ways.

2.3.3 Following notification, the [nominated senior person/ role] will open an incident log and make an initial assessment of the breach’s severity.

2.3.4 The report should capture as much information needed to establish the scope of a breach, but there will be a need to obtain additional information about the event, the assets affected, determining the type of incident, its category and priority before putting together an incident response plan to manage the incident.

2.3.5 This is achieved by interviewing the key personnel involved in the breach and their line managers and collecting as much information as possible to determine how

the breach occurred, what actions have been taken, whether outside agencies are involved and whether the data subjects have been notified.

2.3.6 Some instances will be false alarms or “near miss” events that do not cause immediate harm to individuals or the organisation. These should still be reported, as analysis of these will allow lessons to be learnt and continual improvement.

LEARN

### 2.4 Reporting

2.4.1 The objective of any breach investigation is to identify what actions the organisation needs to take to first prevent a recurrence of the incident and second to determine whether the incident needs to be reported to the Information Commissioner’s Office within the 72 hours’ time limit (for data Bewbush Community Nursery is the Data Controller). Data breaches involving data for which Bewbush Community Nursery is the Data Processor, the data controller will be notified immediately.

2.4.2 The purpose of the report is to document the circumstances of the breach, what actions have been taken, what recommendations have been made and whether the disciplinary action process needs to be followed.

### 2.5 Lessons Learned

2.5.1 Key to preventing further incidents is ensuring the organisation learns from an incident. Review meetings will take place to agree recommendations and each Breach Report will be shared with the appropriate managers and staff.

### 2.6 Review and Revision

2.6.1 This document will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

## 3. OUTLINE PROCEDURE FOR INCIDENT HANDLING

3.1 Investigation

3.1.1 Once a breach has been reported in the form of Annex A, the following actions must be carried out by the [nominated senior person/ role] as soon as possible:

* Create an entry in the Data Breach Incident Log (created by the Annex A form) using the information provided by the reporter
* Create a Data Breach incident number and assign to the log
* Start an investigation report and save it as an attachment to the incident log along with any relevant emails.

3.1.2 Consideration must be given to notifying the individual(s) affected by the breach. Factors to consider include:

* Sensitivity of Information
* Volume of information
* Likelihood of unauthorised use
* Impact on individual(s)

3.1.3 Any notification must be agreed by senior managers.

3.1.4 Begin investigation and complete report as soon as possible

## 4 INCIDENT REVIEWS

4.1 A key part of data protection breach management is a process of continual review. A senior management meeting will provide an update on the progress of any investigation, discuss possible recommendations and consider whether specific incidents should be reported to the ICO.

4.2 These meetings will also review the outcome of any investigations, as appropriate, and examine the recommendations made and discuss information governance matters affecting the company.

## 5 RECOMMENDATIONS

5.1 Regardless of the type and severity of incident, there will always be recommendations to be made even if it is only to reinforce existing procedures.

5.2 There are two categories of recommendation that can be made:

* Local – these apply purely to the department(s) affected by the incident and will usually reflect measures that need to be taken to restrict the chances of the same type of incident occurring.
* Corporate – some incidents will be caused by factors that are not unique to one department but can be found right across the organisation.

5.3 Issues such as training, information handling and physical security affect all facets and it is essential that the organisation identifies such risks and puts in place measures to prevent the incident occurring elsewhere.

5.4 All recommendations will be assigned an owner and have a timescale by when they should be implemented which has a dual purpose. The first is to ensure that the organisation puts in place whatever measures have been identified and that there is an individual that can report back on progress. The second is that where incidents are reported to the ICO, the company can demonstrate that the measures have either been put in place or that there is a documented plan to do so.

5.5 The Identification of vulnerabilities and the production of recommendations is a reactive but necessary process. The ability for the organisation to accrue the knowledge of what has happened together with the impact is a fundamental part of learning which can then be disseminated throughout the organisation and beyond.

**Annex A – Data Protection Breach Reporting Form**

The aim of this document is to ensure that in the event of a security incident such as data loss, all information can be gathered to understand the impact of the incident and what must be done to reduce any risk to customers and/or Bewbush Community Nursery data and information and the individuals concerned.

The checklist can be completed by anyone with knowledge of the incident. It will also require review by the (Senior Manager) and the Data Protection Officer who can determine the GDPR implications and assess whether changes are required to existing business processes.

1.

|  |  |
| --- | --- |
| Summary of Incident |  |
| Date and Time of Incident |  |
| Number of people whose data is affected |  |
| Nature of breach e.g. theft/disclosed in error/technical problems |  |
| Description of how breach occurred |  |

2.

|  |  |
| --- | --- |
| When was breach reported? |  |
| How you became aware of the breach? |  |
| Has the (senior manager) and Data Protection Officer been informed |  |

3.

|  |  |
| --- | --- |
| Full description of personal data involved (without identifiers) |  |
| Number of individuals affected |  |
| Have all affected individuals been informed? |  |
| If not, state why not:Is there any evidence to date that the personal data involved in this incident has been inappropriately processed or further disclosed?If so, please provide details: |  |

4.

|  |  |
| --- | --- |
| What immediate remedial action was taken? |  |
| Has the data been retrieved or deleted? |  |
| If yes - date and time. |  |

5.

|  |  |
| --- | --- |
| Describe the risk of harm to the individual as a result of this incident |  |
| Describe the risk of identity fraud as a result of this incident |  |

6.

|  |  |
| --- | --- |
| Have you received a formal complaint from any individual affected by this breach? If so, provide details? |  |

7.

|  |  |
| --- | --- |
| Do you consider the employee(s) involved has breached information governances policies and procedures? |  |
| Please inform of any disciplinary action taken in relation to the employee(s) involved. |  |
| Had the employee(s) completed data protection training? |  |
| As a result of this incident, do you consider whether any other personal data held may be exposed to similar vulnerabilities? If so, what steps have been taken to address this? |  |
| Has there been any media coverage of the incident? If so, please provide details. |  |
| What further action has been taken to minimise the possibility of a repeat of such an incident? Please provide copies of any internal correspondence regarding any changes in procedure? |  |