Human Resources

Data Security Breach Management Policy

IMS-HRD-013

Version: 1.00

2016-03-002

Data Security Breach Management Policy

1. Index

Data Security Breach Management Policy

2. Introduction

For the purposes of this policy Kibble Education and Care Centre and all associated companies will be referred to as Kibble.

Kibble has a responsibility under the Data Protection Act 1998 to ensure appropriate and proportionate security is in place for the personal data it holds. This responsibility is recognised as a vital business function and is underpinned by the eight principles of the Data Protection Act 1998.

This policy establishes and formalises the procedures for dealing with a data security breach.

3. Scope

This policy applies to all services within Kibble and all associated companies.

- The policy covers all personal data held, maintained and used in all locations and in all formats (paper and electronic including emails).
- The policy applies to all Kibble staff, volunteers, contractors and consultants that access and/or use Kibble information.
- The policy includes and covers any data sharing agreements current or future.
- The policy applies to all third parties, current or future, that process, manage or store personal data on Kibble's behalf

4. Aim

The aim of this policy is to clearly communicate the procedures Kibble has in place for dealing with data breaches ensuring compliance with the Data Protection Act 1998 and all supporting/complimentary legislation.

Data Security Breach Management Policy

5. Data Breach Procedures

If a data security breach does occur, staff should follow the procedure set out below:

1. Immediately notify the Kibble Data Protection Officer (DPO) or in his absence the Support Services Manager, include in the notification the following:

    a. The nature of the breach i.e. has the data been lost, shared or stolen
    b. The amount of data involved
    c. How many people are/will be affected
    d. The content of the information.

In addition you should inform the DPO of any steps you have taken to contain or recover the breach.

2. The DPO will offer guidance on any immediate actions that requires to be taken.
3. The DPO will commence the process to begin an investigation.
4. The DPO will set out a detailed action plan.

Data Security Breach Management Policy

6 Investigation and Action Planning

The investigation and action plan will deal with the following:

6.1 Containment and Recovery	
Who initially needs to be made aware of the breach	
Any resources needed to support the investigation	
Any resources need to execute a containment exercise if applicable	
How can the breach be dealt with	
Is there anything that can be done to limit any damage	
Do the police need to be informed	

6.2 Assessing the Risks	
What type of data is involved	
How sensitive is the data	
If data has been lost or stolen, is the data encrypted	
What has happened to the data	
What could the data tell a third party about the individual	
How many individuals' personal data are affected by the breach	
Who are the individuals affected	
What harm could come to those individuals	
Are there any wider consequences to the loss	
Do we need to contact banks to assist in preventing fraudulent use	

6.3 Notification of Breaches	
Notify the individual(s) affected.	
If the breach has been contained and the DPO's investigation concluded they should be advised of this.	
If not contained and investigation is on-going they should be informed of this and what immediate steps have been taken to contain the situation	
Consider notification to the Information Commissioners Office (see appendix 1)	
Are there any other agencies/ bodies that need to be notified	

6.4 Evaluation and Response	
Evaluate the risks and where they lie	
How can the risks be minimised	
Has the breach identified any weaknesses in security measures, how can this be rectified	
Are staff aware of their duties, is further training needed	

The investigation and any remedial action should be fully documented and kept centrally by the DPO.

Data Security Breach Management Policy

7 Guidance on Reporting Breaches

There is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, however the Information Commissioners believes serious breaches should be brought to the attention of their Offices

There is no clear definition of a serious breach however the following should be used as guidance to inform the decision on whether to report.

Potential harm to individuals	Is there significant actual or potential harm as a result of the breach, if so, the recommendation is to report	Report
Volume of the data involved	Where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm the recommendation is to report.	Report
Sensitivity of the data	Where small amounts of personal data are involved where the release could cause a significant risk of individuals suffering substantial harm. This is most likely to be the case where that data is sensitive personal data as defined in section 2 of the DPA. A	Report

If unsure whether to report or not, then the recommendation is to report.

8 Reporting Breaches

8.1 Making the report

Where the DPO decides that a report should be made to the ICO is should be done as follows:

By email at:

Scotland@ico.org.uk

or by letter to:

The Information Commissioners office – Scotland
45 Melville Street
Edinburgh
EH3 7HL

8.2 The notification should include:

- The type of information and number of records
- The circumstances of the loss/release/corruption
- Action taken to minimise/mitigate effect on individuals involved including whether they have been informed
- Details of how the breach is being investigated
- Whether any other regulatory body has been informed and their response
- Remedial action taken to prevent future occurrence
- Any other information you feel may assist us in making an assessment

8.3 What will the Information Commissioner's Office do when a breach is reported?

The nature and seriousness of the breach and the adequacy of any remedial action will be assessed and a course of action determined. They may:

- Record the breach and take no further action
- Investigate the circumstances of the breach and any remedial action which could lead to:

  i. no further action
  ii. a requirement on the data controller to undertake a course of action to prevent further breaches
  iii. formal enforcement action turning such a requirement into a legal obligation
  iv. Where there is evidence of a serious breach of the DPA, whether deliberate or negligent a monetary penalty of an amount determined by the Commissioner up to the value of £500,000.