

Human Resources

Data Security Breach Management Policy

IMSHRD013

Version: 1.00

Disclaimer

While we do our best to ensure that the information contained in this document is accurate and up to date when it was printed please refer to the electronic copy on the intranet for the latest version.

If you require further clarification on our document control system, please contact the Quality Assurance Department.

2016 03 002

Data Security Breach Management Policy

1. Index

1. INDEX.....	1
2. INTRODUCTION.....	2
3. SCOPE.....	2
4. AIM.....	2
5. DATA BREACH PROCEDURES.....	3
6 INVESTIGATION AND ACTION PLANNING.....	4
6.1 ContainmentandRecovery.....	4
6.2 Assessingthe Risks.....	4
6.3 Notificationof Breaches.....	4
6.4 EvaluationandResponse.....	4
7 GUIDANCE ON REPORTING BREACHES.....	5
8 REPORTING BREACHES.....	6
8.1 Makingthe report.....	6
8.2 Thenotification shouldinclude:.....	6
8.3 What will the Information Commissioner’s Office do when a breach is reported?.....	6

~~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

DocumentNumber
KRNumber

IMSHRD013
201603002

DocumentNumber
KRNumber
CurrentRevision

IMSHRD013
201603002
1.00

Data Security Beach Management Plan

