Guidance on Data Security Breach Management

Information Assurance Group

April 2016

Version 2

Based on the Information Commissioner's Office (ICO) Guidance on data security breach management under the Data Protection Act

Document Control Sheet

Name of Document:	Guidance on data security breach management
Author	Alison Morris, Records and Heritage Manager
Consultees	Information Assurance Group: including: Graham Jarvis, Head of Lifelong Learning, Culture and Sport Sean Hoath, Senior Solicitor Mike Alexander, ICT Security Officer Atholl Scott, Internal Audit Manager Sheila Campbell, Principal Librarian
Description of Content	Guidance on data security breach management - based on the ICO guidance on data security breach management
Distribution:	Council wide upon approval
Status	Version 2
Date	28th April 2016 (previous 5th June 2015)

Contents

1.0 Introduction

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

The Moray Council (TMC) is the Data Controller for all information it handles. TMC's Nominated Representative is Graham Jarvis, Head of Lifelong Learning, Culture and Sport, who chairs the Information Assurance Group

2.0 First Action

Report the breach to line or department manager(s) as soon as the breach has been identified. Managers should inform Graham Jarvis as soon as possible of every breach, and then complete the Data Breach Reporting Form (see appendix 1).

Graham Jarvis will then establish a team to investigate and manage the breach. This may include the following personnel as appropriate:-

- Chair will be appointed by the Data Controller representative and the Service Lead.
- Data Controller – Graham Jarvis, Head of Lifelong Learning, Culture and Sport
- Legal Services – Sean Hoath, Senior Solicitor
- Records Management – Alison Morris, Records and Heritage Manager
- ICT Security – Mike Alexander, ICT Security Officer
- Service Lead(s) – usually a line or departmental manager(s)
- Others as identified

This team will manage the four main areas of the breach management plan.

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response/report

3.0 Containment and Recovery

Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will involve input from specialists across the business such as ICT, HR and legal as appropriate, and, in some cases contact with external stakeholders and suppliers.

Consider the following:

1. Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise.
2. Establish whether there is anything we can do to recover any losses and limit the damage the breach can cause.
3. Where appropriate inform our partners (Police, NHS etc)

4.0 Assessing the Risks

Before deciding on what steps are necessary further to immediate containment, assess the risks that may be associated with the breach:-

- potential adverse consequences for individuals
- how serious or substantial these are
- how likely they are to happen and what the impact(s) is likely to be

Also consider:-

- What type of data is involved?
  - How sensitive is it? Remember that some data is sensitive because of its very personal nature (health and social care records) while other data types are sensitive because of what might happen if it is misused (bank account details)
- If data has been lost or stolen, are there any protections in place such as encryption that would mitigate the risks?
- What has happened to the data?
  - Could it be used for purposes that are harmful to the individuals to whom the data relates?
  - What could the data tell a third party about the individual(s)?

Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of the data subject.

- How many individuals' personal data are affected by the breach?
  - It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but it is certainly an important determining factor in the overall risk assessment
  - Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach
- What harm can come to those individuals?
  - Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their lives?
  - Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service we provide?
  - If individuals' bank details have been lost, consider contacting the Council's bank for advice on anything they can do to help prevent fraudulent use.

5.0 Notification of Breaches

Notification will be done once approved by Graham Jarvis.

5.1 Notifying those involved – individuals and organisations

Informing people and organisations that we have experienced a data security breach can be an important element in our breach management strategy.

Answering the following questions will assist in deciding whether to notify organisations or individuals who have been affected by the breach:

- Can notification help meet security obligations with regard to the seventh data protection principle on information security?
- Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information we provide to mitigate risks, for example by cancelling a credit card or changing a password?
- Consider how notification can be made appropriately for particular groups of individuals, for example, if the breach involves children or vulnerable adults.
- Have we considered the consequences of 'over notifying'. Not every incident will warrant notification.

We also need to consider who to notify, what we are going to tell them and how we are going to communicate the message. This will depend to a large extent on the nature of the breach but the following points may be relevant to our decision:

- Make sure we notify the appropriate regulatory body, if appropriate. A sector specific regulator may require us to notify them of any type of breach. The Information Commissioner's Office should only be notified when the breach involves personal data
- There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation
- Our notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what we have already done to respond to the risks posed by the breach
- When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what we are willing to do to help them
- Provide a way in which they can contact us for further information or to ask us questions about what has occurred – this could be a helpline number or a web page, for example.
- Consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions, as appropriate to the circumstances. Consult contracts and Information Sharing Protocols (ISPs) to verify if there is a requirement to notify specific partners in such situations.

5.2 Notifying the Information Commissioner's Office (ICO)

If a large number of people are affected or there are potentially very serious consequences the Moray Council will inform the ICO. Notification will only be done through Graham Jarvis.

When notifying the ICO include details of the security measures in place such as encryption and, where appropriate, details of the security procedures in place at the time the breach occurred. We should also inform the ICO if media are aware of the breach so that we can manage any increase in enquiries from the public.

The ICO's Data Protection Breach Notification Form is available at https://ico.org.uk/for-organisations/report-a-security-breach/ and will require TMC's registration number: Z7512703.

The ICO has produced guidance for organisations on the information expected to be given as part of a breach notification and on what organisations can expect from the ICO on receipt of notification. This guidance is available on their website: http://www.ico.org.uk

5.3 Informing the Media

Advise Graham Jarvis who will co-ordinate the response with the press officer.

When informing the media, it is useful to inform them whether we have contacted the ICO and what action is being taken. ICO will not normally tell the media or other third parties about a breach notified to them, but they may advise that this is done.

6.0 Evaluation and Response/Report

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of the response to it.

The following points will assist managers in evaluating existing risks:

- Make sure the council knows what personal data is held, where and how it is stored. Establish where the biggest risks lie. For example, how much sensitive personal data does the council have? Is this data stored across the business or is it concentrated in one location?
- Risks will arise when sharing with, or disclosing to, others especially if ISPs are not agreed. TMC should make sure that transmission methods are secure and we only share or disclose the minimum amount of data. By doing this, even if a breach occurs, the risks are reduced.
- Identify weak points in our existing security measures such as using portable storage devices, access to public networks, taking paper documents to meetings, home working and such like.
- Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice.

- Consider whether the Council needs to establish a group of technical and non technical staff who discuss 'what if' scenarios – this would highlight risks and weaknesses as well as giving staff at different levels the opportunity to suggest solutions.
- Refer to TMC's Business Continuity Plan for dealing with serious incidents, consider implementing a similar plan for data security breaches http://intranet.moray.gov.uk/documents/Chief_Executive/business_continuity_policy.pdf

The evaluation will be reported back to the Information Assurance Group and actions pursued.

7.0 Contacts

The Information Assurance Group:

Graham Jarvis, Head of Lifelong Learning, Culture and Sport (Chair)
01343 563365 (Ext: 3365) graham.jarvis@moray.gov.uk

Alison Morris, Records & Heritage Manager
01343 562633 (Ext. 2633) alison.morris@moray.gov.uk

Sean Hoath, Senior Solicitor
01343 563077 (Ext: 3077) sean.hoath@moray.gov.uk

Mike Alexander, ICT Security Officer
01343 563445 (Ext: 3445) mike.alexander@moray.gov.uk

Atholl Scott, Internal Audit Manager
01343 563055 (Ext: 3055) atholl.scott@moray.gov.uk

Sheila Campbell, Principal Librarian
01343 562610 (Ext: 2610) sheila.campbell@moray.gov.uk

Appendix 1

Data Breach Reporting Form

The purpose of this form is to capture instances where the security of personal information has been compromised so that appropriate protective/corrective measures can be put in place.

The breach should be instantly reported to Graham Jarvis, Head of Lifelong Learning, Culture and Sport (01343 563365 Graham.Jarvis@moray.gov.uk). This form should be completed by line managers and passed to Graham to record the current information known.

More information is available: Intranet > Reference > Information Security

Describe the Incident	
What data or personal information was involved?	
How was this compromised?	
Was any actual harm caused?	
Has any disciplinary action been taken against staff?	
Has a contractual remedy been used against a contractor (where the contractor has compromised Council data)?	
What follow up action has been identified? Has this been followed up?	
Further information: e.g. has a complaint been received?	

Completed by:

Name:

Job Title:

Date:

Received by:

Name:

Job Title:

Date: