Argyll and Bute Council

Data Protection - Breach Notification Procedure

Date	Version	Owner
25/10/17	0.1	Head of Governance and Law
20/03/18	0.2	Head of Governance and Law
25/05/18	Final	Head of Governance and Law

May 2018

1. Introduction

1.1 The aim of this procedure is to provide;

a) a clear understanding of the Council's obligations in terms of current data protection legislation in relation to data breaches

b) a basis to ensure that any potential data breaches are addressed in a timely and appropriate manner including containing the impact of any breaches, minimising the risk associated with the breach and determining what action is necessary to secure personal data and prevent further breaches.

1.2 The Council holds, processes, and shares a large amount of personal data, a valuable asset that needs to be suitably protected.

1.3 The Council has a legal duty to protect personal data from incidents which may lead to a data protection breach that could compromise security. Such a breach may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

1.4 This procedure relates to all personal and sensitive data held by the Council regardless of format. Similarly it applies to all staff employed by the Council, including temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the Council.

1.5 This procedure should be read in reference to the Council's current Data Protection Policy and the Data Protection and Information Security Handbook.

2. Data Breaches

2.1 For the purpose of this procedure, data security breaches include both confirmed and suspected incidents.

2.2 An incident in the context of this procedure is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately and has caused or has the potential to cause damage to the Council's information assets and /or its reputation.

2.3 An incident includes but is not restricted to, the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)
- Equipment theft or failure

- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

2.4 A data breach therefore occurs when data is lost, stolen, inappropriately accessed or damaged. In these circumstances the incident must be properly investigated and reported and all action necessary to rectify the situation must be implemented.

3. Reporting an incident

3.1 Any individual who accesses, uses or manages the Council's information is responsible for reporting data breaches and information security incidents immediately to their line manager who must then verify and escalate the matter to the Data Breach Group via email to databreach@argyll-bute.gov.uk

3.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

3.3 The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process. See **Appendix 1**

3.4 All staff should be aware that any breach of the Data Protection Act may result in the Council's Disciplinary Procedures being instigated.

4. Containment and Recovery

4.1 The Data Breach Group will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

4.2 An initial assessment will be made by the Data Breach Group in liaison with other relevant officers to establish the severity of the breach and who will take the role of investigating officer in relation to the breach.

4.3 The investigating officer will establish whether there is anything that can be done to recover any losses and limit the damage the breach

could cause.

4.4 The investigating officer will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

4.5 The investigating officer, in liaison with the Data Breach Group will determine the suitable course of action to be taken to ensure a resolution to the incident.

5. Investigation and Risk Assessment

5.1 An investigation will be undertaken by the nominated investigating officer immediately and wherever possible within 24 hours of the breach being discovered/reported.

5.2 The investigating officer will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

5.3 The investigation will need to take into account the following:

- the type and sensitivity of the data involved
- any protections in place (e.g. encryptions)
- what has happened to the data e.g. has it been lost or stolen
- whether the data could be used illegally or inappropriately
- the identity and number of individuals involved and the potential effects on them e.g. whether there are wider consequences to the breach

6. Notification

6.1 The Data Breach Group must always be advised of the breach and the Data Protection Officer in consultation with the Head of Governance and Law and the Executive Director of Customer Services will ensure that further notification is given to the Chief Executive and Information Commissioner as required.

6.2 Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- whether there are any legal/contractual notification requirements;
- whether notification would assist the individual affected – could they act on the information to mitigate risks?
- whether notification would help prevent the unauthorised or unlawful use of personal data?
- would notification help the Council meet its obligations under the seventh data protection principle;

- if a large number of people are affected, or there are very serious consequences, whether the Information Commissioner's Office (ICO) should be notified. The ICO will only be notified if personal data is involved. Guidance on when and how to notify ICO is available from their website at: https://ico.org.uk/media/1536/breach_reporting.pdf
- the dangers of over notifying, not every incident warrants notification and over notification may cause disproportionate enquiries and work.

6.3 Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the Council for further information or to ask questions on what has occurred.

6.4 The Data Breach Group must consider notifying third parties such as the police, insurers, bank or trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

6.5 The Data Breach Group must also consider whether the Communications Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

6.6 All actions taken in relation to the breach will be recorded by the Data Breach Group.

7. Evaluation and response

7.1 Once the initial incident is contained, the Data Breach Group will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

7.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

7.3 The review will consider:

- where and how personal data is held and where and how it is stored
- where the biggest risks lie, and will identify any further potential weak points within its existing measures
- whether methods of transmission are secure; sharing minimum amount of data necessary
- identifying weak points within existing security measures

- staff awareness
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security

7.4 If deemed necessary a report recommending any changes to systems, policies and procedures will be prepared for consideration by Strategic Management Team.

DATA BREACH GROUP

Douglas Hendry, Executive Director, Customer Services – (01546 604244)

Charles Reppke, Head of Governance and Law – (01546 604192)

Judy Orr, Head of Customer and Support Services – (01586 555280)

Iain Jackson, Governance and Risk Manager – (01546 604188)

Gerry Wilson, ICT and Digital Manager – (01436 658936)

Andy Hubbard, ICT Compliance and Security Officer – (01436 658980)

John McVey, ICT Production Manager – (01546 604486)

Katrina Duncan, ICT Project and Liaison Manager – (01436 658938)

Gerry McDonald, ICT Networks and Server Manager – (01436 658979)

Kate Connelly, Solicitor – (01546 604166)

APPENDIX 1: DATA BREACH REPORT FORM

Please act promptly to report any data breaches.

If you discover a data breach, you must;

- ✓ notify your line manager immediately
- ✓ the line manager must complete Section 1 of this form
- ✓ email it to databreach@argyll-bute.gov.uk

Section 1: **Notification of Data Security Breach**	**To be completed by officer reporting the incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	

To be completed by Governance and Law	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Investigating Officer in consultation with the in liaison with the Data Breach Group**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the University or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK Personal Data Special Category personal data (as defined in the Data Protection Act)	

relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) health, sex life or sexual orientation; e) genetic or biometric data	
Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
Personal information relating to vulnerable adults and children;	
Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
Spreadsheets of information about individual cases of employee discipline or sensitive negotiations which could adversely affect individuals.	
Security information that would compromise the safety of individuals if disclosed.	
The Head of Governance and Law in consultation with the Director of Customer Services to consider whether it should be escalated to the Strategic Management Team	

Section 3: Action taken	**To be completed by the Investigating Officer in consultation with the Data Breach Group**

Incident number	
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	Yes/No If YES, notified on (date):
Follow up action required/recommended:	
Reported to Data Protection Officer and Lead Officer on (date):	
Reported to other internal stakeholders (details, dates):	
To be completed by Governance and Law	
Notification to ICO	YES/NO If YES, notified on: Details:
Notification to data subjects	YES/NO If YES, notified on: Details:
Notification to other external, regulator/stakeholder	YES/NO If YES, notified on: Details: