Data Security Breach – Guidance and Management Advice	**15 November 2016**
Corporate Policy and Resources Committee	**For Decision**

Linkage to Council Strategy (2015-19)	
Strategic Theme	Leader and Champion
Outcome	Provide civic leadership to our citizens
Lead Officer	Head of Policy and Community Planning
Cost: (If applicable)	

1.0 Introduction

1.1 A Council is required, under the Data Protection Act 1998, to ensure the security and protection of personal information, particularly sensitive personal information.

1.2 Causeway Coast and Glens Borough Council will make every effort to avoid the unauthorised or unlawful processing of data or the accidental loss, destruction or damage to personal information. However, it is possible, as has been seen from recent experiences within some major organisations, that there could be a data breach for whatever reason.

1.3 If this occurs it is important that staff know what they need to do once they become of the data breach, particularly as the Information Commissioner has the power to impose fines of up to £500,000 for serious data breaches.

2.0 Proposed Guidance and Management Advice on Data Breaches

2.1 This draft document (copy attached) outlines the action required of senior Council Officers in the event of a data breach. It covers the issue of containment of the breach, investigations that need to be undertaken, and the assessment of risk both to the Council as well as potential adverse consequences for individuals affected by the data breach.

2.2 The document also outlines when it may be appropriate to escalate the matter by reporting it to the PSNI and the Information Commissioners Office.

2.3 The final section of the document outlines the process of evaluating the effectiveness of Council's response to the data security breach and what action needs to be taken, eg weaknesses that need to be addressed.

3.0 Recommendation

It is recommended that the Corporate Policy and Resources Committee recommend to Council approval of the draft document "Data Security Breach – Guidance and Management".

DATA PROTECTION ACT 1998

Data Security Breach - Guidance and Management

Version Control

Version	Author / Reviewer	Review Date	Amendments
2.1	Linda R McKee	February 2016	Draft. SIRO terminology inserted
2.2	Linda R McKee, Patrick McColgan, David Hunter	15 June 2016	Draft – ICT input
2.3	Elaine Kirk	22 August 2016	Appendix edited to remove contacts for Pinsent Masons.
2.4	Internal Auditor	August 2016	Reference made to data breach register and incorporation of appendix in body of guidance.
2.5	Elizabeth Beattie	07 Sept 2016	Various amendments in relation to role of SMT
2.6	ISMG	11 October 2016	Amendments considered and agreed to progress

Introduction

Causeway Coast and Glens Borough Council will make every effort to avoid breaches of the Data Protection Act and in particular the loss of personal data.

The Council will take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. However, it is possible that a data security breach will occur. What is important in these circumstances is that the Council responds appropriately.

It is important that members of staff know what to do if they become aware of a data breach and that management know how to contain and risk assess the loss of data.

The Information Commissioner has the power to fine authorities up to **£500,000** which is due to increase under new legislation for the most serious data breaches.

Such fines are likely if an initial breach is not handled appropriately or if the breach was considered foreseeable.

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

- 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.

Any member of staff who becomes aware that there has been a data security breach is responsible for reporting it ***immediately*** to their line manager.

Action Required in the Event of a Data Security Breach

1. Containment and Recovery

Any member of staff who becomes aware that there has been a data security breach is responsible for reporting it ***immediately*** to their line manager, who should inform their Head of Service.

The Head of Service should determine and record:

- the data affected
- how many individuals' records have been disclosed / or are affected
- the current situation – has the breach been contained and if not, how many people have access to the affected data
- what action has been taken to resolve the breach
- how and when the breach happened

- whether there have been similar occurrences previously
- any other relevant details.

The Head of Service should report the breach immediately by email and phone to the Heads of Policy and ICT and also to the relevant Director / Directorate Head. It should also be sent to the Information Governance Office. The subject line should read: “Data breach report – urgent”.

The Information Governance Officer will record the incident in the data breach register.

Note: If the incident is an ICT Security incident, the procedure should be in accordance with the ICT Security Incident Policy and Procedure.

The Heads of Policy and ICT, along with the relevant Head of Service, will investigate and work to contain the situation and draw up a recovery plan to include any damage limitation.

They will take steps to investigate and will:

- establish who needs to be made aware of the breach and the need for confidentiality
- limit communication to an agreed group to avoid any unintended waiver of privilege or other unplanned disclosure of information
- ensure a clear communication strategy with a central point of contact.
- secure any evidence
- establish whether there is anything to be done to recover any losses and limit the damage the breach could cause

2. Assessment of Risks

Before deciding on further steps beyond those already taken, the Heads of Policy / ICT (in consultation with the relevant Head of Service) will assess the associated risks.

It is important to assess the potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen. The following factors should be considered:

- What type of data is involved?
- How sensitive is it?
- 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?
- Who are the individuals whose data has been breached?

- What harm can come to those individuals? Are there risks of identity theft, physical safety, reputation, financial loss or a combination of these?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence?

3. Consideration of Further Notification

The Senior Information Risk Owner (SIRO) will be notified of the data security breach as soon as possible and will be given details of the containment/recovery activities undertaken and the assessment of risk.

The Senior Information Risk Owner will be responsible for advising the Senior Management Team

Where appropriate the decision to inform individuals affected by the breach, the Police and Information Commissioners Office, etc., will be made by the Senior Management Team (with advice sought from the Head of Policy and Head of ICT if required). Consideration should be given to the following:

- Are there any legal or contractual requirements? (**Note:** legal input will be required to consider whether any privileged investigation is required and maybe required with any notification to any regulators / affected persons).
- Can notification help the Council meet its security obligations with regard to the seventh data protection principle (Personal Information must be secure)?
- Can notification help the individual manage the risks for example by cancelling a credit card, or changing a password?
- How can notification be made appropriate for particular groups of individuals, for example, children or vulnerable adults.
- Who will the Council notify those affected - what will they be told and how will the message be communicated i.e. letter, email, press release, web page?
- Who else should be notified, for example, third parties such as the police, insurers, professional bodies, bank or credit card companies? (**Note**: late notification can be grounds for an insurer to fail to indemnify).
- What is the “line to take” for use with the media? Is it a proactive or reactive approach?

4. Evaluation and Response

It is important not only to investigate the causes of any data security breach but also to evaluate the effectiveness of the Council’s response to it. To this end, the Chair of the Information Security and Management Group will convene the Group to undertake an evaluation of why the incident occurred and how it was handled. The relevant Head of Service will be requested to participate.

The evaluation will take into account the following key issues:

- Can the Council satisfy itself that it knows what personal data is held and where and how it is stored?
- In relation to personal data what and where are the biggest risks for the institution? For example how is “sensitive personal data” being held?
- Are the risks associated with the sharing or disclosing of data suitably identified and managed?
- What are the potential weak points in the Council’s current security measures - such as the use of portable storage devices?
- Ensure that staff awareness of security issues is monitored and identify if there are any gaps required to be filled through training or tailored advice.
- Advice to the Officer responsible for the data and consider if any disciplinary action is required.
- Ensure the data breach register is updated.

On completion of the investigation the Chair will submit a full report to the Senior Information Risk Owner (SIRO) including any recommendations which may include action in accordance with the Council’s Disciplinary Procedures.