Appendix 2(e) # DATA PROTECTION PROCEDURES

5. How to handle a significant data breach

Introduction

Belfast City Council (BCC) will gather and retain a large volume of personal data, some of which is sensitive as defined within the Act. This data is lawfully processed to ensure BCC meets its statutory obligations with proper technical / organisational measures put in place to protect it.

Unfortunately there may be an occasion when data is lost or inappropriately released. It is therefore essential BCC have a procedure in place whereby quick and necessary action is invoked to minimise any risk or damage to an individual and the Council.

The lack of a data breach procedure creates a risk for BCC, data subjects and any organisation with whom it interacts. A breach may result in reduced trust, reputational damage, lost revenue and substantial costs associated with resolving the matter.

Purpose

This guidance sets out the procedure to be followed by all BCC Staff in the event of a significant Data Protection Breach. All data breaches must be reported to Information Governance Unit to allow an assessment of the significance of the breach to be made and to determine whether it is necessary to report it to the Information Commissioner's Office.

Legal Background

The Data Protection Act 1998 regulates the processing of personal data relating to a living individual. It provides a set of rules within the principles of the Act pertaining to the obtaining, holding, use and disclosure of data.

Principle 7 of the Act states that organisations who process personal data must take "appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

A breach of this principle can occur in many forms e.g.

- The loss or theft of data
- Equipment failure
- Professional hacking attempt
- Professional "blagging" whereby data is obtained by deceit.
- Human error by accidental disclosure. An organisation mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address,

Steps to follow upon the discovery of a Data Breach

There are four key steps to consider when responding to a breach or suspected breach:

Step 1: Contain the breach and carryout a preliminary assessment

Step 2: Evaluate the risks associated with the breach

Step 3: Consider who to notify either data subjects and or the ICO

Step 4: Prevent future breaches

As soon as a data breach is discovered or occurs, the staff member concerned should report the available details to his/her line manager, who in turn will escalate the report to the Head of Department. Full and comprehensive details must be presented at this stage to RMU.

If a breach occurs outside normal working hours, the line managers and departmental heads must be informed as soon as possible thereafter. A full data breach incident log should be commenced to provide a documented record of the sequence of events together with actions taken and by whom. See Template 5.1.

If a significant breach occurs, a response team should be immediately organised by the Town Solicitor involving key Council staff. The following individuals within BCC must be informed immediately and one person from this team should be identified to lead on the investigation;

Head of Digital Services
Records Manager
Corporate Communications Manager
Town Solicitor
Appropriate Head of Section
Minute taker / Log keeper

Consideration must be given at an early stage to inform the Police Service of Northern Ireland (PSNI) if the data has been lost / stolen or if the data may pose a risk or impact on the safety of any individual concerned. This maybe very relevant if BCC owned electronic devices including Laptops, tablets, moblile phones etc are involved and confidential data is held within them.

Each data breach will be considered on a case by case basis and on the specific circumstances. An assessment must be made by the above persons to determine what course of action must be taken and the following points reviewed:

- The nature of the data involved
- The sensitivity of the data e.g. health, finance, security etc
- Has the data been lost or stolen?
- Is there any encryption or protection afforded to the data?
- What use could the data be to anyone?
- Could the data be used to harm, damage or cause distress to any individual concerned
- The number of data subjects involved
- Who are the data subjects e.g. staff, councillors, members of the public, clients and suppliers
- Are there risks to their safety or reputation or financial loss
- Is there a wider risk to public health or confidence in any service provided by the Council?
- Do any Council information systems require immediate closure?
- Can the data involved by replicated?

At this stage, BCC must consider whether to inform those persons affected by the breach. The seriousness of the situation will obviously have a bearing on how quickly this should be done. A response should be compiled covering how and when the breach occurred and also to provide reassurance and advice to the individuals affected.

A decision must then be made (based on the circumstances) as to how each individual is informed, either face to face, by telephone or in writing. A detailed record must be kept if and when this is done.

This initial contact should be carried out by a senior officer who has knowledge of the breach. Questions will be asked by those contacted and the above person must be in a position properly answer these and respond appropriately. This will be carried out to also enable the individuals concerned to take protective measures and take necessary action if credit cards or banking data require cancelling or passwords and PIN numbers need changed.

The lead person investigating the breach should now consider whether the Information Commissioner's Office (ICO) should be informed. Not every breach will require ICO notification and the following points will assist in deciding:

- The number of persons affected
- The nature of the personal data
- The potential impact that could have on the individuals
- Has any data been recovered or likely to be recovered?
- Is legal action required via the Court?
- Is the media aware of the breach?

If a decision is made to inform the ICO, the Template 5.2 form must be used.

The report will 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.

BCC will always treat any breach as a serious matter and the lead person will carry out a full and detailed investigation. Once that has been completed, the reason for the data breach together with any recommended remedial action will be identified and reported to senior management.

Any recommendations or directions from the ICO will be considered and acted upon if required.

Implementation

It is the responsibility of Heads of Service/Directors to ensure their staff are made aware of this procedure and the obligations contained within it. This procedure will be highlighted as part of the overall Data Protection awareness training delivered to all Belfast City Council staff. Further advice and guidance can be obtained from the Information Governance Unit.

Monitoring & Review

This procedure will be subject to internal review one year from its implementation and annually thereafter.

Template 5.1 – Data Breach Communications Log

Data Breach Communications Log			
Date	Time	Who	Description / Outcome

Template 5.2 – Data Breach Notification to ICO

Data Breach Notification Form to the Information Commissioner

Please provide as much information as possible. If you don't know the answer, or you are waiting on completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant information, e.g. incident reports.

1	What is the name of your organisation (the data controller)?	
2	Who should we contact if we require further details concerning the incident? (Name and job title, email address, contact telephone number and postal address)	
3	Have you notified as a data controller? If so please provide your registration number.	
4	Have you reported any previous incidents to the ICO? If so, please provide brief details and reference numbers, where known.	
5	When did this incident occur?	
6	Briefly describe the incident.	
7	Has any personal data been placed at risk? If so, please give us an outline of what this data consists of.	
8	Approximately how many data subjects have been affected?	
9	Have you informed the data subjects that this incident has occurred?	
10	Has there been any media coverage of the incident?	
11	Have you taken any action to minimise/mitigate the effect on the data subjects involved? If so please	

	provide brief details.	
12	Are you carrying out an investigation into the incident - If so when will you complete it and what format will it take?	
13	Have you informed any other regulatory body of the matter? If so please provide their details and an outline of their response.	
14	What action have you taken to prevent similar incidents in the future?	
15	Is there any other information you feel would be helpful to the ICO's assessment of this incident?	

Sending this form

Send your completed form to casework@ico.gsi.gov.uk, with 'Security breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please note that we cannot guarantee security of forms sent by email.

What happens next?

When the ICO receives this form, they will contact BCC within seven calendar days to provide:

- a case reference number; and
- an explanation of what to expect during their investigation of the incident.

If you need any help in completing this form, please contact Belfast City Council Information Governance Unit.