Ashfield
DISTRICT COUNCIL

Data Protection Breach Procedure

January 2019

Contents:

1. Introduction

1.1 The Data Protection Act 2018 (DPA) in conjunction with the General Data Protection Regulation (GDPR), is based around six principles of 'good information handling'. These give people specific rights in relation to their personal information and place certain obligations on Ashfield District Council (the 'Council') who are responsible for processing it.

1.2 Anyone who processes personal data in the Council is bound by the DPA 2018 and the GDPR.

1.3 Processing data means obtaining, recording and holding personal data and performing any operation on the data, including the erasure/destruction of the data.

1.4 Personal data is defined as information which relates to a living individual who can be identified from the data or from other information which is in possession of, or is likely to come into the possession of, the data controller. The information may be in the either electronic or manual format. The data may be a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. For example, this will include:

- A name and address;
- information attached to a reference number that could be used to identify someone directly or indirectly;
- a company e-mail address if it includes a person's name

1.5 A data protection breach is where data is lost, damaged, destroyed, stolen, misused and/or accessed unlawfully.

Principle 6 states:
The sixth data protection principle is that personal data must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

1.6 Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

1.7 Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

1.8 Everyone has a responsibility to ensure that personal data is only used for lawful purposes and to ensure that data is kept secure and not accessed for personal reasons. It is a criminal offence to misuse personal data, which may result in a criminal investigation/prosecution against the individual (staff member) concerned.

2. Purpose and Scope

2.1 The Council is obliged under Data Protection legislation, the GDPR and related EU and national legislation to have in place a framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

2.2 This document sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the Council.

2.3 This procedure relates to all personal and special categories (sensitive) data held by the Council regardless of format.

2.4 This procedure applies to all staff at the Council. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the Council.

2.5 The objective of this procedure is to contain any breaches, to minimise and mitigate the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

3. Definitions / Types of breach

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

3.2 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 reputation or cause loss, damage or distress to an individual.

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

- Theft of data or equipment on which data is stored
- Loss of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Accidental Loss
- Destruction of personal data
- Damage to personal data
- Equipment failure
- Unlawful disclosure of personal data to a third party
- Unauthorised use of, access to or modification of information systems, for example, accessing Council systems for personal use.

- 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.

4. Reporting an incident

4.1 Any individual who accesses, uses or manages the Council's information is responsible for reporting any suspected or actual data breach and information security incidents.

4.2 If you discover that data has been lost, or if you believe there has been a breach of the data protection principles in the way that data is handled, you must immediately or no later than within 24 hours of first coming to notice, inform the Data Protection Officer (at DPO@Ashfield.gov.uk) and IT Services (at ithelpdesk@ashfield.gov.uk), who must follow the Information Commissioners Office (ICO) guidelines on notification and recording of the breach. The priority must then be to close or contain the breach to mitigate/minimise the risks to those individuals affected by it. If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

4.3 The report must 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 (refer to Appendix 1).

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

5. Containment and recovery

5.1 The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, appropriate steps will be identified and taken immediately to minimise the effect of the breach.

5.2 An initial assessment will be made by the DPO in liaison with relevant officer(s) to establish the severity of the breach and who will take the lead investigating the breach, the Lead Investigation Officer (this will depend on the nature of the breach; in some cases it could be the DPO).

5.3 The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to mitigate the breach, to recover any losses and limit the damage the breach could cause.

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

5.5 Advice from experts across the Council may be sought in resolving the incident promptly.

5.6 The LIO, in liaison with the DPO and relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

6. Investigation and risk assessment

6.1 An investigation will be undertaken by the LIO immediately and wherever possible, within 24 hours of the breach being discovered / reported and the DPO informed.

6.2 The LIO 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. Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause and inform senior management as appropriate.

6.2.1 Levels of risks can be different and vary on each individual breach of data depending upon what is lost/damaged/stolen. For example

- If a laptop is damaged beyond repair then the risk is low as all data can be recovered from a backup.
- If a case file is lost then risks are different depending on what the file contained, the type of data and its sensitivity and the potential adverse consequences for individuals.

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

- the type of data involved;
- its sensitivity;
- the 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 put to any illegal or inappropriate use;
- data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);
- whether there are wider consequences to 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 life;
- are there wider consequences to consider such as a risk to life;
- loss of public confidence in an important service you provide;
- regardless of what has happened to the data, what could the data tell a third party about the individual; 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 other people.

7. Notification

7.1 The LIO and / or the DPO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible. The LIO and/or the DPO will also determine whether the affected individuals should be notified of the breach.

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

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation, please see Individual Rights: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/
- whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);
- whether notification would help prevent the unauthorised or unlawful use of personal data;
- whether there are any legal / contractual notification requirements;
- the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

7.3 Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification 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.

7.4 The LIO and / or the DPO must consider notifying third parties such as the police, insurers, banks or credit card companies, and 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.

7.5 The LIO and/ or the DPO will consider whether the Communications Team should be informed regarding a press release and be ready to handle any incoming press enquiries.

7.6 A central record in Legal Services will be kept of any personal data breach, regardless of whether notification to the ICO was required.

8 Evaluation and response

8.1 Once the initial incident is contained, the DPO 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.

8.2 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.

8.3 The review will consider:

- where and how personal data is held and where and how it is stored;
- where the biggest risks lie including identifying potential weak points within existing security measures;
- whether methods of transmission are secure; sharing minimum amount of data necessary;
- staff awareness;
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

8.4 If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Council.

9. Procedure Review

1.9 This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

Data Protection Breach Incident Reporting Form – to be sent to the Data Protection officer with 24 hours to DPO@ashfield.gov.uk

Contact Details of Person Submitting Form	
Name	
Job Title	
Address	
Telephone Number	
Email Address	
Incident Information	
Date and Time of Breach	
Date and Time Breach Detected	
Who / What Reported the Breach	
Description and type of the Breach	
The likelihood and severity of the resulting risk to people's rights and freedoms. i.e. Could result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination,	

identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.”	
Approximate Number of Data Subjects Affected	
Details of any ICT Systems Involved	
Details of Action taken to Mitigate Effect on Data Subjects	
Who is Aware of Breach	
Date notified to DPO	

For DPO use only

Date received by DPO	
The likelihood and severity of the resulting risk to people’s rights and freedoms.	
Inform ICO Yes/No	
Date of informing ICO and details of person spoken to and ref no (if provided)	
If not reported, why not	

Conclusion, after investigation	
Date of informing ICO of conclusion. after investigation and details of person spoken to and ref no (if provided)	
Signed off by	
Date signed off	