East Herts District Council

Data Breach Policy

Document Control

Organisation	East Hertfordshire District Council
Title	Data Breach Policy
Author – name and title	Tyron Suddes, Information Governance and Data Protection Manager
Owner – name and title	Tyron Suddes, Information Governance and Data Protection Manager
Date	
Approvals	
Version	1.1
Next Review Date	

Contents

1. Introduction

This Policy sets out the obligations of East Hertfordshire District Council ("the Council") regarding the handling and reporting of data breaches and personal data breaches in accordance with UK Data Protection Legislation. "Data Protection Legislation", in this Policy, means all legislation and regulations in force from time to time regulating the use of personal data including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, and any successor legislation.

The UK GDPR defines "Personal Data" as any information relating to an identified or identifiable natural person (a "Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The UK GDPR defines a "Personal Data Breach" as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

The Council is under a duty to report certain types of Personal Data Breach directly to the Information Commissioner's Office ("ICO"). The Council is also required to inform individual Data Subjects in the case of breaches that present a high risk of adversely affecting their rights and freedoms.

All personal data collected, held, and processed by the council will be handled in accordance with the Council's Policy for Handling Personal Data.

The Council has in place procedures for the detection, investigation, and reporting of data breaches. This Policy applies to all data breaches (including personal data breaches) within the Council and is designed to assist in both the handling of such breaches and in determining whether or not they must be reported to the ICO and/or to Data Subjects.

The Council's Information Governance and Data Protection Manager and Information Officer are responsible for overseeing the handling of all data breaches. The Council's Leadership Team, line managers and Information Governance and Data Protection Manager are responsible for the implementation of this Policy and ensuring that this Policy is adhered to by all staff.

2. Scope of Policy

1.1 This Policy relates to all forms of data (including personal data and sensitive personal data (known as "special category" under the Data Protection Legislation)) collected, held, and processed by the Council.

1.2 This Policy applies to all staff and elected members of the Council, including but not limited to employees, agents, contractors, consultants, temporary staff, casual or agency staff, or other suppliers or data processors working for or on behalf of the Council.

1.3 This Policy applies to all data breaches, whether suspected or confirmed.

2. Data Breaches

2.1 For the purposes of this Policy, a data breach means any event or action (accidental or deliberate) which presents a threat to the security, integrity, confidentiality, or availability of data.

2.2 Incidents to which this Policy applies may include, but not be limited to:

2.2.1 the loss or theft of a physical data record;

2.2.2 the loss or theft of computer equipment (e.g. laptop), mobile devices (e.g. smartphone or tablet), portable data storage devices (e.g. USB drive), or other data storage devices;

2.2.3 equipment failure;

2.2.4 unauthorised access to, use of, or modification of data (or inadequate access controls allowing unauthorised access, use, or modification);

2.2.5 unauthorised disclosure of data;

2.2.6 human error (e.g. sending data to the wrong recipient);

2.2.7 unforeseen circumstances such as fire or flood;

2.2.8 hacking, phishing, and other 'blagging" offences whereby information is obtained by deception;

3. Internal Reporting

3.1 If a data breach is discovered or suspected, members of staff should immediately notify their line manager and complete a Staff Data Breach Report Form (available on the Council's intranet) and send the completed form to the Council's Information Officer and/or Information Governance and Data Protection Manager. If considered necessary due to the nature of the breach, it should be reported to IT Services via the ICT Help Desk (ext. 2249).

3.2 Members should complete a Staff Data Breach Report form and send the completed form to the Council's Information Officer and/or Information Governance and Data Protection Manager and if considered necessary, IT should be notified.

3.3 A completed Staff Data Breach Report Form should include full and accurate details about the incident including, but not limited to (where applicable):

3.3.1 the time and date the breach was discovered;

3.3.2 the type(s) of data involved;

3.3.3 where the breach involves personal data, the categories(s) of data subject to which the personal data relates (e.g. customers, employees etc.);

3.3.4 whether or not any sensitive personal data is involved;

3.3.5 how many Data Subjects are likely to be affected (if known);

3.3.6 details of what may have caused the breach;

3.3.7 details of any immediate actions taken to reduce the impact of the breach.

3.4 If a data breach occurs or is discovered outside of normal working hours, it should be reported as soon as is reasonably practicable to keep within the **72 hour limit** imposed by Data Protection Legislation. Staff should keep in mind that some time may be needed to minimise the effect of the potential data breach.

3.5 Unless and until instructed to by the Information Governance and Data Protection Manager or a Head of Service, no further action should be taken with respect to a data breach. In particular, individual members of staff should not take it upon themselves to notify affected Data Subjects, the ICO, or any other individuals or organisations.

4. Initial Management and Recording

4.1 Upon receipt of a Staff Data Breach Report Form (or upon being notified of a data breach in any other way), the Information Governance and Data Protection Manager and/or Information Officer and relevant member(s) of staff and/or their line manager shall begin by determining whether the data breach is still occurring. If this is the case, appropriate steps shall be taken immediately to minimise the effects of the data breach and to stop it.

4.2 Having established the above, the following steps shall then be taken by the parties mentioned in 5.1 above with respect to the data breach:

4.2.1 undertake an initial assessment of the data breach, liaising with the relevant staff and departments where appropriate, to establish the likelihood and severity of the data breach. This is will be determined on a case by case basis and may include, but is not limited to, consideration of the number of Data Subjects and sensitivity of personal data involved;

4.2.2 With assistance from IT if required, contain the data breach and, to the extent reasonably practicable, recover, amend, or restrict the availability of (e.g. by changing or revoking access permissions or by temporarily making the data unavailable electronically) the affected data;

4.2.3 determine whether anything further can be done to recover the data and/or other losses, and to limit the damage caused by the breach;

4.2.4 establish who needs to be notified initially (including, if physical records or equipment have been lost or stolen, the police) as part of the initial containment;

4.2.5 determine, in liaison with the relevant staff and departments, the best course of action to resolve and remedy the data breach; and

4.2.6 record the breach and the initial steps taken above in the Council's Data Breach Log.

4.2.7 Having completed the initial steps described above, the Information Governance and Data Protection Manager and/or Information Officer and relevant member(s) of staff and/or line manager shall proceed with investigating and assessing the data breach as described in Part 5, below.

5. Investigation and Assessment

5.1 The Information Governance and Data Protection Manager and/or Information Officer and relevant member(s) of staff and/or line manager shall begin an investigation of a data breach as soon as is reasonably possible after receiving a Staff Data Breach Report Form (or being notified in any other way) and, in any event, within **24 hours** of the data breach being discovered and/or reported.

5.2 Investigations and assessments may take the following into account:

5.2.1 the type(s) of data involved (and, in particular, whether the data is personal data or sensitive personal data);

5.2.2 the sensitivity of the data (both commercially and personally);

5.2.3 what the data breach involved;

5.2.4 what organisational and technical measures were in place to protect the data;

5.2.5 what might be done with the data as a result of a breach (including unlawful or otherwise inappropriate misuse);

5.2.6 where personal data is involved, what that personal data could tell a third party about the Data Subjects to whom the data relates;

5.2.7 the category or categories of data subject to whom any personal data relates;

5.2.8 the number of Data Subjects (or approximate number if calculating an exact number is not reasonably practicable) likely to be affected by the data breach;

5.2.9 the potential effects on the Data Subjects involved;

5.2.10 the potential consequences for the Council;

5.2.11 the broader consequences of the data breach, both for Data Subjects and for the Council;

5.3 The results of the investigation and assessment described above must be recorded in a Data Breach Report and a summary noted in the Council's Data Breach Log.

5.4 Having completed the investigation and assessment described above, the Information Governance and Data Protection Manager and/or Information Officer in liaison with the relevant member(s) of staff and/or line manager**,** shall determine the parties to be notified of the breach as described in Part 6, below.

6. Notification

6.1 If not already aware, the Head of Service of the affected service area shall be made aware of all data breaches regardless of the level of risk.

6.2 The Information Governance and Data Protection Manager and/or Information Officer in liaison with the relevant member of staff and/or line manager shall determine whether to notify one or more of the following parties of the breach:

6.2.1 Senior Information Risk Officer (SIRO);

6.2.2 Deputy Chief Executive and/or Chief Executive

6.2.3 affected Data Subjects;

6.2.4 the ICO;

6.2.5 the police;

6.2.6 affected third parties;

6.2.7 IT (if not already notified).

6.3 When considering whether to notify the SIRO, Deputy Chief Executive, Chief Executive or affected third parties, the nature of the breach and the severity of the impact it may have on Data Subjects should be taken into account. All data breaches deemed medium to high risk should immediately be brought to the attention of these parties. The Council's Leadership Team and Audit and Governance Committee will be made aware of all data breaches regardless of risk level on a half yearly basis through a data breach summary report.

6.4 When considering whether (and how) to notify individual Data Subjects in the event of a personal data breach, the following should be considered:

6.4.1 the likelihood that Data Subjects' rights and freedoms as set out in the Data Protection Legislation (and the Council's Policy for Handling Personal Data) will be adversely affected;

6.4.2 whether there is a legal or contractual requirement to notify;

6.4.3 whether measures in place to protect the affected personal data (e.g. pseudonymisation or encryption) have been applied, thereby rendering the data unusable to any unauthorised parties;

6.4.4 whether measures have been taken following the data breach that will ensure that a high risk to the rights and freedoms of affected Data Subjects is no longer likely to occur;

6.4.5 the benefits to Data Subjects' of being notified (e.g. giving them the opportunity to mitigate the risks posed by the data breach);

6.4.6 whether notifying individuals will involve disproportionate effort (in which case a public communication or other widely available notice may suffice, provided that affected Data Subjects will still be informed effectively);

6.4.7 the best way of notifying Data Subjects, taking into account the urgency of the situation and the security of the possible methods;

6.4.8 any special considerations applicable to certain categories of data subject (e.g. children or vulnerable people);

6.4.9 the information that should be provided to affected Data Subjects;

6.4.10 how to make it easy for affected Data Subjects to contact the Council to find out more about the data breach;

6.4.11 further assistance that the Council should provide to the affected Data Subjects, where appropriate;

6.4.12 the risks of over-notifying – not all data breaches require notification and excessive notification may result in disproportionate work and numbers of enquiries from individuals;

6.5 When individual Data Subjects are to be informed of a data breach, those individuals must be informed of the breach without undue delay. Individuals shall be provided with the following information:

6.5.1 a user-friendly description of the data breach, including how and when it occurred, the personal data involved, and the likely consequences;

6.5.2 clear and specific advice, where relevant, on the steps individuals can take to protect themselves;

6.5.3 a description of the measures taken (or proposed to be taken) to address the data breach including, where relevant, measures taken to mitigate any possible adverse effects;

6.5.4 contact details for Information Governance and Data Protection Manager and relevant member(s) of staff from whom affected individuals can obtain further information about the data breach.

6.6 When considering whether (and how) to notify the ICO of a data breach, the following should be considered:

6.6.1 the risk and potential harm to Data Subjects, their rights, and freedoms – harm can include (but is not limited to) financial harm, physical harm, loss of control over personal data, discrimination, identity theft or fraud, damage to reputation, and emotional distress;

6.6.2 the volume of personal data involved – the ICO should be notified if a large volume of data is involved and there is a real risk of Data Subjects suffering harm as a result, however it may also be appropriate to notify the ICO if a smaller amount of high-risk data is involved;

6.6.3 the sensitivity of the data involved – the more sensitive the personal data is, the less the volume of it is relevant and if the data breach presents a significant risk of Data Subjects suffering substantial detriment or distress, the ICO should be notified.

6.7 If the ICO is to be notified of a data breach, this must be done within **72 hours** of becoming aware of the breach, where feasible. This time limit applies even if complete details of the data breach are not yet available. The ICO must be provided with the following information:

6.7.1 the category or categories and the approximate number of data subject whose personal data is affected by the data breach;

6.7.2 the category or categories and the approximate number of personal data records involved;

6.7.3 the name and contact details of the Information Governance and Data Protection Manager from which the ICO can obtain further information about the data breach;

6.7.4 a description of the likely consequences of the data breach; and

6.7.5 a description of the measures taken (or proposed to be taken) to address the data breach including, where relevant, measures taken to mitigate any possible adverse effects.

6.8 The police may have been contacted at an earlier point in the data breach procedure (see 4.2), however further investigation may reveal that the data breach resulted from a criminal act, in which case the police should be further informed.

6.9 Records must be kept of all data breaches, regardless of whether notification is required. The decision-making process surrounding notification should be documented and recorded in a Data Breach Report and a summary noted in the Data Breach Log.

7. Evaluation and Response

7.1 When the steps set out above have been completed, the data breach has been contained, and all necessary parties notified, the Information Governance and Data Protection Manager and/or Information Officer and/or relevant member(s) of staff, their line manager and, if required, the relevant Head of Service shall conduct a complete review of the causes of the data breach, the effectiveness of the measures taken in response, and whether any systems, policies, or procedures can be changed to prevent data breaches from occurring in the future. Additionally, where breaches have not been escalated, these will be reported via the half yearly meetings as mentioned in paragraph 6.3 above in order to determine if improvement is required. Any recommendations and/or actions made through a review, if applicable, will be shared with all council staff as soon as possible.

7.2 Such reviews shall, in particular, consider the following with respect to data (and in particular, personal data) collected, held, and processed by the Council:

7.2.1 where and how data is held and stored;

7.2.2 the current organisational and technical security measures in place to protect data and the risks and possible weaknesses of those measures;

7.2.3 the methods of data transmission for both physical and electronic data and whether or not such methods are secure;

7.2.4 the level of data sharing that takes place and whether or not that level is necessary;

7.2.5 whether any data protection impact assessments need to be conducted or updated;

7.2.6 staff awareness and training concerning data protection;

7.3 Where possible improvements and/or other changes are identified, the Information Governance and Data Protection Manager shall liaise with the relevant member(s) of staff, their line manager and, if required, the relevant Head of Service with respect to the implementation of such improvements and/or changes.

7.4 Any actions taken against an employee found to be responsible for a confirmed data breach shall be in line with the Council's Disciplinary Policy and should be treated as a general misconduct breach of the Council's Code of Conduct.