HARLOW COUNCIL
Data Security Breach Management Policy

Document Information

Policy Author(s):	**Marie Bentley and Declan White**	Document Version No:	**0.1**
Approved and authorised:		Document Version Date:	
Date authorised:		Document Type:	**Policy**
Service(s)	**Governance and Finance**	Department(s)	**Corporate Information and ICT**

1. Introduction

Harlow District Council is registered with the Information Commissioner as a Data Controller – an organisation that processes personal data. All Data Controllers have a responsibility under the Data Protection Act 1998 (DPA) to comply with the requirements of Principle 7.

Principle 7 of the DPA states that organisations which 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".

No organisation handling personal information can guarantee that it will never experience losses but by ensuring that standards are equivalent to, or exceed, best practice, data subjects will be reassured that all reasonable steps are taken to preserve and protect their information. This Policy provides a consistent framework to be followed by all Harlow Council employees for reporting and investigating any breaches of the DPA.

2. Scope of policy

The Council is obliged under DPA to have in place a framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

Council staff will process personal data as part of their job and must adhere to the DPA 1998. A breach may result in the Council being liable in law for the consequences of the breach.

The objective of this Policy is to contain any breaches of the Act, to minimise the risks associated with the breach and to consider what action is necessary to secure personal data and prevent further breaches.

This Policy is based on guidance issued by the Information Commissioner's Office (ICO).

3. Policy Statement

All users of personal data within the Council have a responsibility to ensure that they process such data in accordance with the DPA and the eight Data Protection Principles.

The Principles are that personal data must be:

1. fairly and lawfully processed;
2. processed for limited purposes;
3. adequate, relevant and not excessive;
4. accurate;
5. not kept for longer than is necessary;
6. processed in line with the individual's rights;
7. secure; and
8. not transferred to countries outside the European Economic Area without adequate protection.

Any breach of the Act by staff constitutes an offence. Such offences will be treated extremely seriously and may constitute a disciplinary offence under the disciplinary procedure, up to and including dismissal. Any employee, who has a concern about processing or storing personal information, is urged to contact the Corporate Information Manager.

All breaches, for example unauthorised or unlawful processing or accidental loss, must be reported so that the appropriate measures can be taken to limit the damage to the individual or individuals and to protect the Council from loss of public confidence.

From time to time individuals may approach the Council expressing concern over the handling of their personal data. The Council's Data Protection Officer will investigate such concerns to determine if the individual is invoking their right to prevent processing likely to cause damage or distress under Section 10 of the Data Protection Act or if a complaint is being made and/or if a breach has occurred.

4. Procedure

A data breach can occur for a variety of reasons, for example:

a) Loss or theft of data or equipment on which data is stored
b) Inappropriate access controls allowing unauthorised use
c) Equipment failure
d) Human error
e) Unforeseen circumstances such as a fire or flood
f) Hacking attack on the Council's ICT systems
g) 'Blagging' offences where information is obtained by deceit
h) Loss of paper records

4.1. What to do when a breach occurs

All staff must report any breaches to their Line Manager and the Senior ICT Manager via the ICT Service Desk (ext 6789). If the breach is discovered outside normal working hours, this should begin as soon as is practicable.

When reporting an incident the following information should be provided:

a) Date of incident.
b) Location of incident.
c) Nature of incident, e.g. is it a loss, theft, disposal, unauthorised disclosure?
d) Nature of data involved - list all data elements, e.g. whether it is names, files, dates of birth or reference number.
e) What security protection was on the data? Is it protection by a password, encryption or something else?
f) Is there any backup of the data, if so where?
g) Number of people potentially affected, an estimate should be provided if no precise figure can be given.
h) Details of any steps taken to retrieve data or to contain the breach if it is involved unauthorised access or potentially compromised security.

4.2. How will the breach be dealt with?

The Council has set up an Information Security Management Group (ISMG). The group consists of the following Officers, Senior Information Risk Officer (Head of Finance), Data Protection Officer (Head of Governance),Senior ICT Manager and the Corporate Information Manager. The Senior ICT Manager is responsible for informing members of the ISMG about the breach.

The Head of Service where the breach has occurred should take the lead on investigating the breach with the support of the ISMG.

Appropriate government departments and support teams will be informed about network security breaches.

The CMT, HR Manager, Legal Services Manager and the Communications Team should be notified by the ISMG, depending on the relevance and severity of the breach.

The Line Manager of the Service Area will discuss the matter with 'staff' responsible for the breach. If negligence is proven, appropriate disciplinary action could be taken. Training and tailored advice will be provided by the ISMG.

To limit damages, the Head of Service or if delegated the Line Manager, will establish whether there is anything that can be done to recover any losses that the breach can or might have caused. These could include making arrangements to isolate or close a compromised section of the network, recall any erroneously sent email and find a lost piece of equipment.

The ISMG will provide advice and co-ordinate with the Head of Service on steps to be taken.

The ISMG, when appropriate**,** will notify all staff in the Council about the breach and action taken.

The Head of Service or delegated Line Manager will inform the police, if data, or a device containing data (e.g. laptop), has been stolen and it involves the safety of data subject(s).

The ISMG will notify the Information Commissioner's Office (ICO) in line with guidelines under 'Notification of breaches'. However, discussions with the Chief Executive and / or Chief Operating Officer must take place prior to breaches being notified to the ICO by the ISMG.

The ISMG will maintain an audit trail on what actions have been taken (as expected by the ICO).

The ISMG must be kept informed of progress at all stages.

5. Managing the breach

Data security breach management guidance (Appendix A) has been produced to help managers respond to incidents where the security of personal data may be compromised.

There are four elements to any breach management plan:

a) Containment and recovery
b) Assessment of ongoing risk
c) Notification of breach
d) Evaluation and response

5.1. Containment and recovery

Breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from IT, HR and Legal and in some cases contact with external partners and suppliers.

5.2. Assessing the risks

Certain data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example, where a laptop is irreparably damaged but its files were backed up and can be recovered, albeit at some cost to the Council.

Whilst these types of incidents can still have significant consequences the risks are very different from those posed by, for example, the theft of a customer database, the data on which may be used to commit identity fraud.

Before deciding on what steps are necessary, further to immediate containment, an assessment of the risks which may be associated with the breach must take place.
Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

5.3. Notification of breaches

A part of breach management is to inform relevant staff and individual that there has been a data security breach. However, informing people about a breach is not an end in itself.

Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

Consideration needs to be given to notifying third parties such as the police, insurers, trade unions, professional bodies and bank or credit card companies who can assist in reducing the risk of financial loss to individuals.

Although there is no legal obligation to report breaches to the ICO, the Commissioner believes that serious breaches should be notified. However, the ICO should only be notified by the ISMG when the breach involves personal data and after discussions with the Chief Executive and or the Chief Operating Officer.

5.4. Evaluation and response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of the response to it in case there are systemic or ongoing problems. Perhaps there was a lack of clear allocation of responsibly or inadequate policies or procedures. Monitoring of staff awareness of security issues may reveal gaps that can be filled through tailored advice or training. Risks will arise when sharing data with or disclosing data to others. The storing or transmission of personal data on portable or mobile devices is a weak point in security measures if encryption is not employed. Where the breach is serious, a report will be written by the relevant Head of Service after the investigation is complete detailing mitigating action taken.

6. Additional Information

This Policy should be read in conjunction with other related Council's policies and procedures found on the Council's intranet listed below:

a) Access to Information Policy
b) Records Management Policy
c) Document Retention and Disposal Schedule
d) Corporate Information Security Policy
e) ICT Acceptable Usage Policy

Appendix A

Data Security Breach Management: Guide for Managers

1. Purpose of this guide

This guide is designed to help managers respond to incidents where the security of personal data may have been compromised. It is based on advice provided by the Information Commissioner's Office.

This is not a definitive guide to the Data Protection Act 1998, but will help managers take immediate and appropriate action when they consider that data security may have been breached.

Managers seeking more detailed information on our obligations regarding the processing of personal data should consult Harlow Council's Data Protection (Access to Information Policy), Corporate Information Security and ICT Acceptable Usage policies.

2. Background

The majority of the services Harlow Council delivers involve the use (processing) of personal data. This personal data may be about individuals as users of our services, as employees of the Council, or as elected members (Data Subjects).

Under the Data Protection Act 1998, we are obliged to adhere to principles of good practice which protect the rights of the individuals whose personal data we collect, store and use. The principles state that personal data must:

1. Be processed fairly and lawfully.
2. Be obtained only for one or more specified purposes and not processed in an incompatible manner.
3. Be adequate, relevant and not excessive.
4. Be accurate and, where necessary, kept up to date.
5. Not be kept any longer than necessary.
6. Be processed in accordance with the rights of Data Subjects.
7. Be surrounded by appropriate technical and organisational security.
8. Not be transferred outside of the European Economic Area without adequate protection.

Although we place tight controls on the processing of personal data, we must be prepared to manage any breaches of data security in a timely and efficient manner, to guard against the inappropriate or illegal processing of data and to protect the individuals whose personal data may have been disclosed / accessed.

3. Why do breaches happen?

The security of personal data can be compromised in a variety of ways:

- Human error (e.g. data disclosed to the wrong individual).
- Accidental loss of data (e.g. briefcase left on a train).
- Theft of ICT equipment (e.g. laptop stolen from home).
- Inappropriate use of information systems (e.g. staff with access to a system using the data within it for purposes other than those it should be used for).
- Penetration of ICT security (e.g. hacking).
- Deception (e.g. individuals deceiving the organisation as to their identity in order to access personal data they are not entitled to).

Careful planning helps us identify these areas of potential risk, and Harlow Council has robust processes and systems in place to minimise the possibility that the security of personal data could be breached for any of the reasons above.

However, we must accept that breaches can still happen. In these rare instances, it is important that the organisation takes immediate action to remedy the situation.

4. Who should investigate / manage a breach?

The organisation's immediate response to a suspected data security breach must be to initiate an investigation into the situation and quickly identify and carry out the actions which will limit the damage caused by the breach.

It is important that the right person takes prompt ownership of the situation. In most cases, this will be the Head of Service for the data which has been compromised.

The Head of Service is the person who has responsibility for the collection and processing of the data in question. They will be the person who has made the business case for collecting / processing the data, and will have justified the processing of the data for these purposes in line with the organisation's obligations under the Data Protection Act 1998.

In the event that this responsibility sits at Director level, or above, the breach management role may be delegated further down the line management structure. However, this person must have the authority to make judgements and take decisions on behalf of the service area they represent.

The investigation must be conducted in accordance with the following timetable:

Stage	Action	Timescale
Suspected breach identified	Incident must be reported to Line Manager, Head of Service and the Information Security Management Group (ISMG) via the Senior ICT Manager (ICT Service Desk - ext 6789)	Immediate
Initial assessment of incident	The Head of Service or if delegated, the Line Manager must undertake the initial investigation of the incident to enable ISMG to assess potential harm to individuals and corresponding need to inform the ICO of the breach	Within 48hrs
Full Report completed	The Head of Service or if delegated, the Line Manager must complete the investigation in line with the Manager's Guide	Within 14 days of breach notification
DPT-led review of Report	ISMG will review the report, re-assess the need to notify ICO, and support the organisation in any action planning necessary to prevent a similar occurrence	Within 7 days of receiving full Report

5. Dos and don'ts

If you suspect there has been a breach of data security, it is important to act swiftly and responsibly to manage the situation. However, there can be many competing and conflicting demands to balance in a very short period of time. Remember:

- **Do** give the situation your immediate and full attention.
  - ⇒ *Immediate action can curtail the breach, limit the potential harm to Data Subjects, and identify inappropriate or unsafe activity before further problems occur.*

- **Do** report all potential breaches to the ISMG.
  - ⇒ *Even if you are unsure that the situation constitutes a breach of data security. It is preferable to investigate and conclude that there has not been a breach, than to fail to investigate and risk the possibility of serious harm to Data Subjects or further breaches in the future.*

- **Do** make sure you understand your responsibilities under the *Data Protection Act 1998*.
  - ⇒ *If you are investigating a potential data security breach, you need to understand what obligations the Act places upon us (as an organisation, and as individuals), and how it protects the rights of Data Subjects. The ISMG can advise on any points you are unsure of. The group consists of the following officers, Senior Information Risk Officer (Head of Finance), Data Protection Officer (Head of Governance), Senior ICT Manager and Corporate Information Manager.*

- **Don't** panic.
  - ⇒ *Breaches of data security are serious situations. The best way to resolve them is to remain calm, make considered judgements on appropriate action, and carry out a proper investigation.*

- **Don't** ignore or attempt to conceal the incident.
  - ⇒ *It won't help. You may be breaking the law, and you will be putting the affected Data Subjects at risk. It is important that we learn from any data security breaches and apply this learning to minimise the possibility of future breaches. It is equally important that the people who use our services, or who work for us, can trust us. Failing to take appropriate action in response to a data security breach will damage that trust.*

- **Don't** react impulsively.
  - ⇒ *Swift action is key, but it is important to think before you act. Reacting angrily with the staff who have made you aware of the breach, or with the staff you think may be responsible, may prevent them alerting you of problems in the future. It may also make it difficult for you to discover the true facts of the situation, and hamper your investigation. Be careful in your approach when notifying Data Subjects of a breach; make sure you are passing on clear information which will help people protect their privacy, not causing panic by giving out incomplete or incorrect information before you are in full possession of the facts.*

- **Don't** try and resolve the matter on your own.
  - ⇒ *Always report a suspected breach to the ISMG via the ICT Service Desk (ext 6789), and make sure your Head of Services is kept updated on the situation. The ISMG will provide advice and guidance on your investigation, and will liaise with the Information Commissioner's Office, if appropriate. The ISMG will liaise with CMT, Human Resources Manager, Legal Services Manager and the Communications Team where this is required. The Legal Service will be able to give legal guidance in light of the breach, and the Communications Team will handle any communication with the media.*

6. Five step plan for managing data security breaches

Any potential breach of data security will present its own unique set of issues and problems to address. Follow these five steps when dealing with a potential (or actual) breach:

- ➥ Step 1: Control.
- ➥ Step 2: Data recovery.
- ➥ Step 3: Risk assessment.
- ➥ Step 4: Notification.
- ➥ Step 5: Evaluation.

6.1. Step 1: Control

- Take ownership of the situation.

⇒ *(i.e. manage the breach. If you don't think you are the right person, then tell your Head of Service / Line Manager immediately so that a prompt decision can be taken about who will lead the date breach investigation).*

- Identify any urgent action which must be taken in reaction to the situation.
  ⇒ *(e.g. is immediate action needed to stop further breaches in the same area, do the police need to be notified?).*

- Report the incident to the ISMG and provide as much information as you can about the nature of the breach. Indicate which other teams may need to become involved.
  ⇒ *(e.g. The Legal Service, Communications team, Internal Audit, Human Resources).*

- Control the spread of information about the situation.
  ⇒ *(e.g. who needs to be told, what level of information they need. You must liaise with the Communications Team regarding any media involvement / public statements).*

- Consider what immediate action could limit the damage caused by the breach.
  ⇒ *(e.g. alerting data subjects to the possibility of identity theft and providing advice / support).*

- Ascertain whether there is any early indication of staff misconduct.
  ⇒ *(consider whether immediate disciplinary action / police notification is required).*

6.2. Step 2: Data recovery

- Determine to what extent the data can be recovered. Aim to:
  ⇒ *Recover ICT equipment (e.g. has anything been handed in to the police, lost property of an external company, an HDC office, etc.).*
  ⇒ *Recover hard copy materials (e.g. arrange for return of documents if you know whose possession they are in).*
  ⇒ *Seek advice from the Legal Service when trying to recover data or equipment from third parties.*
  ⇒ *In the event of damage to, or loss of, data in our Information Systems, ensure that Disaster Recovery plans are implemented to guarantee continuity of service.*

6.3. Step 3: Risk assessment

- Assess the potential harm posed to Data Subjects by the breach. Consider:
  ⇒ *What data has been lost / stolen / disclosed?*
  ⇒ *How many Data Subjects could be identified by the breach?*
  ⇒ *What is the nature of our relationship with the Data Subjects (e.g. are they service users, members of staff, elected members, etc.)*
  ⇒ *Was the data confidential / sensitive?*
  ⇒ *What could the data reveal about the Data Subjects it applies to?*
  ⇒ *Was the data protected in any way which would prevent a third party from being able to access it / use it (e.g. software encryption)?*
  ⇒ *What could a third party do with the data, and who could be at risk of harm as a result of this?*

- Assess the potential harm posed to Harlow Council by the breach. Consider:
  ⇒ *Loss of trust in a service / the organisation as a whole.*
  ⇒ *Damage to credibility.*
  ⇒ *Difficulty in encouraging future take up of our services.*
  ⇒ *Damage to the employer / employee relationship.*

- Assess the potential harm to other third parties. Consider:
  ⇒ *Could the data pose a risk to individuals other than the Data Subjects it applies to?*
  ⇒ *Who are these parties (are they individuals, groups, organisations, etc.)*

- Determine mitigating / remedial action in response to these risks.
  ⇒ *What can you do to protect / support parties you have judged to be at risk of harm?*
  ⇒ *What do you need to do to prevent a repeat of this situation? (procedural change, staff training, etc.)*
  ⇒ *Are there any disciplinary issues to pursue?*

- Formulate your action plan in light of your risk assessment.
  - ⇒ *Consider how these risks impact on your need to notify people about the breach.*
  - ⇒ *Discuss your proposed actions with the ISMG and seek their guidance on any issues you are uncertain about.*

6.4. Step 4: Notification

IMPORTANT**:** before any parties are notified, you must check with *Legal Service* to ensure that notification is undertaken is such a way that it does not prejudice any live court proceedings.

- Decide if you need to inform anyone outside the organisation about the breach. Consider:
  - ⇒ *Who you have identified as being at risk of harm as a result of the breach. Could notifying them help them to protect themselves from potential harm?*
  - ⇒ *Do you have a duty to explain the breach to the Data Subjects, even if they are not at risk of harm (e.g. in the interest of maintaining trust)?*
  - ⇒ *Will notifying individuals help you disseminate advice to assist damage limitation?*
  - ⇒ *Are there any regulations which govern your responsibilities regarding notification (specific rules may apply to your service area - check with the Legal Service) and do you have to notify an official / regulatory body?*
  - ⇒ *Is there a contractual relationship which requires you to notify in the event of a breach?*
  - ⇒ *Should the incident be reported to the police?*
  - ⇒ *Should UNISON be made aware?*

- To what extent should you notify? Consider:
  - ⇒ *Will it help to notify when the breach is suspected, but not confirmed?*
  - ⇒ *What are your minimum obligations?*
  - ⇒ *Could notifying more widely than you are strictly required to help you limit damage in light of the breach?*
  - ⇒ *Could notifying too widely increase the possibility of potential harm to Data Subjects?*

- How should you notify? Consider:
  - ⇒ *Does the content of the notification need to be tailored to different audiences / recipients?*
  - ⇒ *How sensitive is the data in the notification? How does this impact on the communication method you should use?*

- What information do you need to share as part of the notification? Where possible, include:
  - ⇒ *An apology (if appropriate).*
  - ⇒ *An explanation of what has happened*
  - ⇒ *An explanation of how the breach occurred.*
  - ⇒ *Whether the breach is suspected or confirmed.*
  - ⇒ *Date / time of the breach.*
  - ⇒ *What data was involved?*
  - ⇒ *What you have already done / will be doing to remedy the situation.*
  - ⇒ *What risks may be posed to the individual by the breach.*
  - ⇒ *What steps the Data Subjects can take to protect themselves.*
  - ⇒ *What you can do to help protect the Data Subjects.*
  - ⇒ *Contact details for questions, problems and complaints.*

- Does the Information Commissioner's Office need to be informed?
  - ⇒ *The ISMG will consider whether or not the ICO needs to be informed, based on the information you provide about the breach.*
  - ⇒ *Where notification is required, the ISMG will take care of this and will liaise with the ICO to provide any further updates on the investigation / findings.*

6.5. Step 5: Evaluation

- Complete your investigation and evaluate your findings.
  - ⇒ *Produce a report / response document (appropriate to the scale / nature of the breach).*

- ⇒ *Have you identified the cause of the breach?*
- ⇒ *Have you identified / implemented appropriate actions to limit damage in light of the breach?*
- ⇒ *Do you have a strategy for addressing problems with internal processes / systems?*
- ⇒ *Have you identified / planned to engage with key stakeholders for relevant processes / systems?*
- ⇒ *Has your investigation uncovered weaknesses / danger points which you / the organisation were previously unaware of?*
- ⇒ *Do you have a strategy for proactively addressing these issues with relevant teams / parties?*
- ⇒ *Is there anything else which could / should have been done prior to the breach which may have prevented it?*

- Review your experiences.
  - ⇒ *Did any internal processes hamper your investigation?*
  - ⇒ *Did anything happen during your investigation / response to the breach which made the situation worse?*
  - ⇒ *Which aspects of your investigation / response were most successful / helpful in tackling the breach and its aftermath?*

- Sign off and feedback.
  - ⇒ *As Line Manager you must share your findings with your Head of Service and the ISMG.*
  - ⇒ *The Head of Service, ISMG will consider / challenge findings and identify any outstanding actions.*
  - ⇒ *ISMG and Head of Service approve final response / report.*
  - ⇒ *Head of Service / Line Manager to implement any outstanding / agreed actions in line with agreed recommendations.*
  - ⇒ *ISMG to update ICO (if required) and Internal Audit.*

- Post investigation review.
  - ⇒ *Head of Service / Line Manager to monitor implementation of their actions and review progress in line with operational / ICO requirements.*

7. Advice and assistance

If you need any advice on the handling of a data security breach, or would like to discuss any aspects of your investigation, please contact the Information Security Management Group (ISMG = Senior Information Risk Officer (Head of Finance), Data Protection Officer (Head of Governance), Senior ICT Manager and Corporate Information Manager.

Revision History

Date of this revision:
Date of next planned revision:

Version No:	Version date	Summary of Changes	Revised by
0.1	11/07/14	Final draft	Marie Bentley and Declan White