The Information Management Team

**Detailed explanation of processes and procedures followed by the Information Management Team when managing Personal Data Breach Incidents**

Personal Data Breach Procedure

**Contents**

[**Introduction** 2](#_Toc522877595)

[**Process Timeline** 4](#_Toc522877596)

[**Reporting an Incident** 5](#_Toc522877597)

[**Who?** 5](#_Toc522877598)

[**When?** 5](#_Toc522877599)

[**What?** 5](#_Toc522877600)

[**TAKING ACTION** 10](#_Toc522877601)

[**Triaging an Incident** 11](#_Toc522877602)

[**Non-Event (NE)** 11](#_Toc522877603)

[**Near-Miss (NM)** 11](#_Toc522877604)

[**Confirmed Loss (CL)** 11](#_Toc522877605)

[**Investigating an Incident** 11](#_Toc522877606)

[**Repatriation of Information Process** 14](#_Toc522877607)

[**Full Investigation Report** 15](#_Toc522877608)

[**Roles and Responsibilities** 16](#_Toc522877609)

Assessing risk and high risk**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** \_18

Record Keeping\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_18

[**Process Maps** 20](#_Toc522877610)

[**Triaging an Incident** 20](#_Toc522877611)

[**A Non-Event Incident** 21](#_Toc522877612)

[**A Near-Miss Incident** 22](#_Toc522877613)

 [**A Confirmed Loss** 23](#_Toc522877614)

## **Introduction**

**Personal Data breach process following a security Incident**

**This document should be used as a reference guide to assist you when you suspect there has been a personal data breach incident. It details the processes which you should follow, including the investigation which is conducted by the Information Management Team (IMT). If you need to report a suspected personal data breach please email** **data.breach@croydon.gov.uk** **or call 0208 604 7777.**

A “personal data breach” is defined in Article 4 (12) of the General Data Protection Regulation (GDPR) 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”. This not only refers to instances where personal data has been lost; it refers to any occasion when there has been a breach of information security principles such as:

* Confidentiality breach – where there is an unauthorised or accidental disclosure of or access to personal data;
* Integrity breach – where there is an unauthorised or accidental alteration of personal data;
* Availability breach – where there is an accidental or unauthorised loss of access to or destruction of personal data.

Personal data breach is a type of security incident, examples of which include:

* Post or emails being sent to the wrong address;
* Lost or stolen paperwork, USB memory sticks or data CDs;
* Lost or stolen laptops, tablet computers or mobile phones;
* Missing files or documents, electronic or hard copy;
* Printers not printing out documents or prints being left at printers;
* When personal information is used for purposes for which it wasn’t collected;
* When personal information on databases or in files is incorrect;
* Incorrectly forwarding sensitive emails;
* Using the “Reply to All” function in Outlook without checking who should have access to the contents of the email trail;
* Loss of availability where personal data is deleted either accidentally or by unauthorised person
* A power failure rendering personal information unavailable
* Network, phishing, malware and other ICT breaches

The IMT is here to help; not apportion blame. The majority of incidents that occur are either due to human error or inefficient business processes. The IMT’s primary concern when dealing with a personal data breach is to contain the breach, recover the personal data and ensure that no harm comes to residents as a result of an incident. The IMT will also ensure that all staff are trained and educated in our procedures and processes and will make sure that the Council’s policies and protocols are robust and adhered to. To achieve this, the IMT, in conjunction with colleagues in service areas, conduct thorough investigations when an incident is reported so that the Council can learn from mistakes and any operational issues can be highlighted.

Officers should raise any concerns which they may have regarding a suspected personal data breach with their managers and/or Information Management Champion immediately, along with the Information Management Team. The IMT are also available to provide guidance around concerns. The Data Protection Act 2018 and the GDPR introduces a duty upon the Council to report certain types of personal data breach within 72 hours of the Council being aware of the incident to the Information Commissioner’s Office (ICO), so do not delay in contacting the IMT.

The Council is considered as having become “aware” of the incident when any service of the Council has a reasonable degree of certainty that a personal breach incident has occurred. It is therefore imperative that any knowledge about any personal data breach incident is immediately brought to the attention of the IMT by contacting them at data.breach@croydon.gov.uk. Delay in notifying the ICO (where appropriate) may lead to a fine being imposed upon the Council.

**Process Timeline**

|  |  |  |
| --- | --- | --- |
| **Action** | **Time** | **Description** |
|  |  |  |
| Incident occurs |  |  |
|  |  |  |
|  |  |  |
| IMT notified of Incident  | 0 hours | The IMT should be notified of the incident immediately by email to data.breach@croydon.gov.uk or telephone 0208 604 7777.  |
|  |  |
|  |  |  |
|  |  |  |
| IMT start investigation |  | The IMT will commence an investigation as soon as it has been notified to ascertain whether there has been a personal data breach. This process will start by contacting the person who has reported the incident. The Head of Service and relevant Director will also be informed of the incident. All incidents of personal data breach will immediately be reported to the Chief Information Officer (CIO) and the Data Protection Officer (DPO) and added to the Data Breach Register.  |
|  |  |
|  |  |
|  |  |  |
|  |  |  |
| DPO/CIO/Caldicott Guardian informed of incident | 24 hours  | Upon notice of a personal data breach incident, the DPO will make a decision whether or not to notify the Information Commissioner’s Office (ICO), in consultation with the CIO and Caldicott Guardian. The ICO will be notified where the personal data breach is likely to result in a risk to the rights and freedom of individuals. The DPO may suggest a notification in phases to the ICO where a breach has become known but the extent of it is not yet known which will be completed following full and comprehensive investigation of the incident by the IMT. The DPO – in consultation with the CIO and Caldicott Guardian – may decide the incident does not require notification to the ICO.  |
| ICO informed |  |
|  |  |  |
|  |  |  |
| Loss Panel arranged |  | The DPO and/or CIO will request the IMT to convene a Loss Panel where the incident has the potential to result in high risk to the data subject(s) (“serious incident”) A Loss Panel could meet virtually. A Loss Panel could also be required for other incidents to address other issues.  |
|  |  |  |
|  |  |  |
| IMT complete preliminary investigation |  | The IMT will complete the preliminary investigation. |
|  |  |  |
|  |  |  |
| Investigation report forwarded to Loss Panel |  | The investigation report will be forwarded to the Loss Panel. |
|  |  |  |
|  |  |  |
| Loss Panel convened | 72 hours | The Loss Panel will be convened to consider the incident and the results of the investigation. The Loss Panel may also request for certain actions to be carried out.  |
|  |  |
|  |  |
|  |  |  |
|  |  |  |
| Information repatriated |   | Any information that is in the possession of the IMT will be handed back to the team to whom it belongs to, where possible.  |
|  |  |
|  |  |  |
|  |  |  |
| Data subject informed |  | Where the Loss Panel establishes that there is a high risk to the rights and freedoms of individuals the Loss Panel will recommend notification to both the individuals. This will be actioned by the service manager. The CIO will also notify the relevant senior officer(s) of the Council. Where the ICO was notified in phases the DPO will update the notification and advise the ICO of the steps taken to contain and recover the compromised personal data (where possible).  |
|  |  |
|  |  |
|  |  |
|  |  |  |
|  |  |  |
| Panel recommendations actioned |  | A time limit will be set by the Loss Panel within which any recommended action will need to be completed by the service manager.  |
|  |  |
|  |  |  |
|  |  |  |
| **Incident Closed**Incident closure recorded on investigation report disseminated, and Data Loss Register updated |  | After all actions have been completed, the Information Manager (IM) will close the incident and update Data Loss Register. Updated investigation report will be forwarded to the person who reported the incident and to the manager responsible for carrying out any recommendations made by the IM and/or the Loss Panel.  |
|  |  |
|  |  |  |
|  |  |  |

**Reporting an Incident**

When an incident occurs, it should be reported immediately to your line manager and/or the IMT at data.breach@croydon.gov.uk. Do not wait for someone else to report the incident; the IMT would rather receive duplicate information than none at all. It is worth noting that if any IT hardware has been lost or stolen, you should also contact the police and get a crime reference number.

When you report an incident to the IMT, only three fundamental questions need to be answered. These are Who, When and What.

**Who?** This provides the IMT with full details of the person who is reporting the incident. This information is required so that the IMT knows who to contact for information when investigating. This will also be one of the individuals whom the IMT contact when any recommendations have been executed (if any) and the incident has been closed following an investigation.

**When?** This provides the IMT with two dates – when the incident occurred and when the incident was reported. This ensures that the IMT carries out any subsequent investigations in a timely manner. It also allows the IMT to identify incidents with similar issues which may have arisen during the same timeframe.

**What?** This is where you provide the IMT with details of the incident. The IMT requests that you provide as much detail as possible, including dates, times, names and locations, as applicable. This is so that the IMT can promptly launch the investigation process and expedite any actions where required.

Below is an example of the information required when reporting a breach.

**ABOUT YOU**

|  |  |
| --- | --- |
| **Your Name** | Please enter your full name below. |
|  |
| **Your Job Title** | Please enter your full job title below. |
|  |
| **Your Department** | Please state below if you are in CED, WCR, DASHH, CFL or Other. |
|  |
| **Your Team/Service** | Please state below what Team and/or Service you work in. |
|  |
| **Your Telephone Number** | Please provide below a contact number on which you can be reached. |
|  |
| **ABOUT THE BREACH** |
| **What has happened?** | Please provide below details of the incident – what happened, what went wrong, and how it happened.  |
|  |

|  |  |
| --- | --- |
| **Was the breach caused by a cyber incident?**  | Yes/No/Don’t know If Yes please advise for cyber Incidents only:Has the confidentiality, integrity and/or availability of your information systems been affected?* Yes
* No
* Don’t Know

If you answer Yes please specify:Impact on your organisation* High - you have lost the ability to provide all critical services to all users
* Medium you have lost the ability to provide critical services to some users
* Low - there is a loss of efficiency but you can still provide all critical services to all users.
* Not yet known
 |
|  |

|  |  |
| --- | --- |
| **(Cyber Incidents only) Recovery Time**  | * High - you have lost the ability to provide all critical services to all users;
* Supplemented – you can predict your recovery time with additional resources;
* Extended - you cannot predict your recovery time, and need extra resources;
* Not recoverable – recovery from incident is not possible (e.g. sensitive data has been shared publicly);
* Not yet known
 |
|  |

|  |  |
| --- | --- |
| **If there has been a delay in reporting this breach please explain why** |  |
|  |

|  |  |
| --- | --- |
| **How did you find out about the breach?**  |  |
| **When did you find out about the breach?**  |  |
| **Date: Time:** |

|  |  |
| --- | --- |
| **When did the breach occur?**  |  |
| Date: **Time:** |

|  |  |
| --- | --- |
| **Provide details about categories of personal data included in the breach (tick all that apply)**  |  |
| * Racial/ethnic origin;
* Political opinions;
* Religious or philosophical beliefs;
* Trade Union membership;
* Sex life;
* Sexual orientation;
* Gender reassignment;
* Health;
* Basic personal identifiers (e.g. name, contact details);
* Identification data (e.g. usernames, passwords);
* Economic/financial data (e.g. credit card numbers, bank details);
* Official documents (e.g. driving licence, passport);
* Location data;
* Genetic/biometric data;
* Criminal convictions/offences;
* Not yet known; or

Other (please specify) |

|  |  |
| --- | --- |
| **How many data subjects could be affected?** |  |
|  |

|  |  |
| --- | --- |
| **Categories of data subjects affected by the breach (tick all that apply)**  |  |
| * Employees;
* Users;
* Subscribers;
* Students;
* Customers or prospective customers;
* Patients;
* Children;
* Vulnerable adults;
* Not yet known;

Other (please specify) |

|  |  |
| --- | --- |
| **Describe the potential consequences of the breach including any risk/actual harm to data subject(s)**  | Please describe the possible impact on the data subjects as a result of the breach (e.g.Identity theft, fraud, manual loss, threat to professional services, physical harm, distress Please state if there has been any actual harm to the data subjects. |
|  |  |
|  |
| **What is the likelihood that data subjects will experience significant consequences as a result of the breach?**  | Very Likely / Likely / Neutral likely nor unlikely / Unlikely / Very Unlikely / Not yet known Please provide details |
|  |

|  |  |
| --- | --- |
| **If there has been a delay in reporting this breach, please explain why**  |  |
|  |

**TAKING ACTION**

|  |  |
| --- | --- |
| **Describe the action taken or proposed to be taken to deal with the personal data breach**  | Include where appropriate, actions you have taken to fix the problem and to mitigate any adverse effects e.g. confirmed that data sent in error has been destroyed, updated passwords, planning information security training. |
|  |

|  |  |
| --- | --- |
| **Where appropriate describe the measures taken to mitigate any possible adverse effects**  |  |
|  |

|  |  |
| --- | --- |
| **Has the data subject(s) been informed about the breach? (Tick all that apply)** |   |
| * Yes we’ve told affected data subjects;
* We’re about to or are in the process of telling data subjects;
* No there are already aware;
* No but we are planning to;
* No we have decided not to;
* We haven’t decided yet if we will tell them or not; and/or
* Something else (please give details below)
 |

|  |  |
| --- | --- |
| **Have you told, or do you plan to tell, any other organisations about the breach?**  | (e.g. The police, other regulators, other supervisory authorities.)Yes / No / Don’t know.If Yes please specify.  |
|  |

**Triaging an Incident**

The triage process will occur after the IMT has gathered enough information to make such a decision. This will initially be based upon the information that the IMT receives on the Information Loss Reporting Form. The IMT may also have to gather further information from relevant individuals and/or teams. It is important to provide as much information as possible as part of the initial report, as this will expedite the process and appropriate actions can then be taken in a timely manner. In the event that there is a personal data breach of personal and/or sensitive information, the IMT will advise the Information Asset Owner if it is appropriate to contact the Data Subject(s) of the loss. Information Asset Owners will also be responsible for contacting the Data Subject if any further information is required from them. Information Asset Owners would normally be the Head of Service.

The incident will be categorised as one of the following:

**Non-Event (NE)** This is an incident where nothing of concern has occurred from an Information Management perspective. There may still be issues which the IMT can advise on, however, the IMT will only log the incident for recording purposes and close it. The person reporting the incident will be notified that the incident has been closed and the reasons behind this decision.

**Near-Miss (NM)** This is an incident, which under slightly different circumstances, may have resulted in a serious loss of control. Each NM incident has the potential to be a serious loss, and therefore the more NM incidents which are reported and rectified, the fewer serious incidents will occur. The events that caused the near miss will be subjected to root cause analysis to identify the processes or training issues that resulted in the NM and highlight factors that may either amplify or ameliorate the result. The incident will be logged for recording purposes

**Confirmed Loss (CL)** This is an incident where the Council has lost control of the information which it holds. These incidents can vary in severity, however, as previously mentioned, the harm, or potential harm to the Council’s residents(s) has to be taken into account. Investigations for CL incidents will be started straight away, and the departmental Information Management Champion, Head of Service and relevant Director will be notified. When required, the Loss Panel will be convened to advice on further actions and any immediate steps which need to be taken.

**Loss Panel** The Loss Panel consists of the CIO, the Data Protection Officer (DPO), and the Caldicott Guardian. The Council’s Information Manager and Information Governance Solicitor provide advice to the panel. The departmental Information Management Champion and the Head of Service for the team responsible for the loss will be required to attend the Loss Panel.

**Investigating an Incident**

The IMT will launch an investigation as soon as an incident is reported, especially if a resident has been impacted. The aim is for the IMT to have interviewed all relevant individuals from the service within 24 hours so as to be able to make an informed decision on any remedial action(s) which need to be taken and any reporting which may be required. For this reason, it is imperative that everyone with a link to the incident make themselves available to the IMT if required. The IMT will be on hand to provide and help and advice on processes.

The investigation will initially focus on what actually happened, including gathering details from all concerned and building a timeline of events. The IMT may conduct several interviews and each step will be logged to provide an audit trail. In most cases, the departmental Information Management Champion will be included in these conversations. A list of all Information Management Champions can be found on the Intranet.

The IMT, with advice from Information Asset Owners and the Information Manager, may agree actions at this stage and may also make short, medium and long term recommendations.

A form like the one below will be filled in for recording purposes:

|  |  |
| --- | --- |
| **Incident summary** | Details of incident |
|  |
|  |  |
| **Investigator(s)** | Person(s) investigating the incident |
|  |
|  |  |
| **Investigation** | Details of investigation |
| Date | Detail |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| **Recommendations** | Recommendations made directly following investigation |
| Action(s) | Responsibility | Deadline | Completed |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

A copy of the full investigation report will be forwarded to the relevant individuals involved in the incident, most likely to be the Head of Service or a Team Manager and will be made available to the person who reported the incident (if different). This will include details of the investigation and list all actions which have been completed, and which remain outstanding. The relevant senior manager(s) will be informed of the recommendations, and will inform the IMT when all actions have been completed. **The Loss Panel**

NM incidents which are repeated or CL incidents which are likely to result in high risk to the rights and freedoms of individuals will be referred to the Loss Panel. The panel will be convened within 48 hours of the incident, and sometimes sooner, depending on the severity of the incident. It is imperative that you attend this meeting if requested to, or that you send an appropriate deputy.

The CIO chairs the Loss Panel and the other standing members who sit on the panel are:

* The Data Protection Officer (DPO)
* The Caldicott Guardian

The Council’s Information Manager and Information Governance Solicitor will provide advice to the panel. The departmental Information Management Champion, the Service Manager for the area where the incident occurred and the investigating Information Officer (IO) will be invited to attend. The Loss Panel will decide if the loss is to be reported to the data subject(s) and may discuss levels of compensation due to data subjects. They will also confirm actions which need to be taken to minimise the impact of the incident and will base these actions on recommendations made by the IMT.

Where possible, the Loss Panel will seek to agree any decisions. In the event that agreement cannot be reached, the CIO will decide.

A form like the one below will be forwarded to all attendees prior to the panel and will contain details of the investigation which has been carried out:

|  |  |
| --- | --- |
| **Attendees** | List of Loss Panel attendees |
| Name | Initials | Role |
| Matthew Wallbridge(Chair) | MW | Chief Information Officer (Chair)  |
| Nick Sherlock | NS | Caldicott Guardian |
| Sandra Herbert | SAH | Data Protection Officer |
| Jonathan Craven | JC  | Information Manager (advisory)  |
| James Derby | JD | Information Governance Solicitor (advisory)  |
|  |
| **Incident summary** | Details of incident |
|  |
|  |  |
| **Investigation** | Details of investigation |
|  |
|  |  |
| **Recommendations** | Recommendations made by Information Management Team |
| Action(s) | Responsibility | Deadline | Completed |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |
| **Agreed Actions** | Actions agreed by panel |
| Incident to be reported to ICO? | Yes / No |
| Action | Responsibility | Deadline | Completed |
|  |  |  |  |
|  |  |  |  |
| Incident to be reported to data subject? |  |  |  |
|  |  |  |  |
|  |
| **Incident closed date** |  |
| **Incident closed by** |  |
| **Job title/role** |  |

**Repatriation of Information Process**

When information is found or handed in to the IMT, it is imperative that this is handed back to the team where it originated. This is because the documents may relate to a live case and missing files may have an adverse effect on a customer. As such, the IMT will record this information in the full investigation report. This allows the IMT to keep a record of what information was handed back and to whom it was handed back to.

The following table shows the steps which the IMT will take to repatriate information with its owner. It is the Information Asset Owner’s responsibility to ensure that IMT are informed of what needs to happen to their information and also to ensure that the action(s) are carried out.

The IMT will ensure that permission is granted for destruction of any information by email from the relevant senior manager(s), or the CIO.

|  |  |  |
| --- | --- | --- |
| **Action** | **Time** | **Description** |
| IMT receive documents | Day 0 | The IMT in receipt of documents belonging to another service. |
| IMT contact relevant team | Day 1 | Upon initial receipt of the documents, IMT will identify the team who owns it and email the manager of the team informing them how they came into possession of the documents and give them a 10 working day deadline to claim the documents. |
|  |  |
| IMT follow-up with Head of Service (HoS) | Day 5 | If after 5 working days there has been no response to the initial email IMT will send a follow up email copying in the Head of Service reminding the team manager of their responsibility over this information and inform them of 5 days left of original 10 working day deadline. |
| IMT chase team (with HoS and Director) | Day 10 | If by the tenth day IMT has not received a response, IMT will send a follow-up email, copying in the relevant Head of Service and Director and will again remind the team of their responsibility. This email they will give them a further 10 working days from the date of the email confirming that on this date the information will be destroyed securely if IMT have not received a response. |
| IMT chase for the final time (with HoS, Director & Exec. Director) | Day 15 | If by day 15 IMT has not received a response, IMT will send a final warning email, copying in the Head of Service, Director and Executive Director. This email will state that if a response is not received within 5 working days then these documents will securely destroyed. |
| Information Securely Destroyed | Day 20 | If on the 20th working day IMT have not received an update, the information will be securely destroyed on the advice of the CIO. An email will be sent to the relevant team with the Head of Service, Director and Executive Director copied in notifying them of the destruction.  |

**Full Investigation Report**

When all recommended actions have been completed following an incident, the incident will be closed. However, some incidents will require the IMT to conduct further investigations into large scale issues. When this occurs, the IMT will produce a full incident investigation report for senior management which will give a thorough explanation of where processes and procedures failed and will make recommendations based on these findings. These investigations will normally involve various Teams and Departments and will often take several months to complete.

The report will be in the same format as the one below.

|  |  |
| --- | --- |
| **Incident summary** | A summary of the incident(s) which lead to the full investigation |
|  |
|  |  |
| **Investigation Summary** | A summary of what was discovered during the investigation |
|  |
|  |  |
| **Full investigation results** | Detailed results of IMT investigation |
|  |
|  |  |
| **Concerns** | Any risks or concerns |
|  |
|  |  |
| **Further Information** | Any further or supporting information |
|  |
|  |  |
| **Recommendations** | IMT recommendations following the investigation |
|  |

**Roles and Responsibilities**

When dealing with data loss incidents, the roles and responsibilities of the IOs, the IM and other senior members of staff may sometimes merge, depending on the nature of the incident and who was involved in the incident. However, one thing will always remain constant:

**It is the responsibility of all staff to report any type of suspected personal data breach incident**

Reporting incidents allows the Council to learn from any untoward events and enables it to implement policies and procedures which will safeguard customers and staff, which in turn will increase efficiencies and streamline processes.

Below is a list of the other responsibilities when dealing with incidents:

|  |  |
| --- | --- |
| Information Officers | * Triaging an incident
* Arranging meetings
* Undertaking investigations
* Making recommendations
* Ensuring correct documentation is prepared
* Maintaining Data Breach Register
* Advising staff on best practice
* Arranging and presenting IM Training
 |
| Information Manager | * Management of loss process
* Advisor to the Loss Panel
* Can overrule any IO, in any matter
* Final say in categorising incidents
* Making recommendations
* Enforcing Actions
* Providing sign-off when closing incidents
* Convening Loss Panel
 |
| Team Manager/Head of Service | * Ensuring staff are appropriately trained in data protection law and information management for their roles and that training is reviewed annually
* Attend the Loss Panel
* Communicate with Data Subjects when necessary
* Responsible for carrying out any recommended actions and notifying IMT of completion
* Ensuring all incidents are reported to the IMT immediately
 |
| Information Management Champions | * Responsible for promoting and driving forward the IM agenda
* Promote IM training and awareness
* First point of contact for IM queries within their respective services.
* Will have a level of authority which enables them to invoke disciplinary procedures for members of staff within their service who do not comply with IM Policies and Procedures
* Attend Loss Panel
 |
| Chief Information Officer | * Chair of the Loss Panel
* Responsible for all the information which the Council holds
* Consultee on whether a notification should be made to the ICO of any reportable incidents
 |
| Data Protection Officer | * Member of the Loss Panel
* Informing and advising the Council on all its data protection obligations
* Monitoring the Council’s compliance with the GDPR
* Act as the contact point for the ICO on issues relating to processing personal data
* Consultee on all data protection impact assessments
* Responsible for final decision on notification to the ICO and informing the ICO of any incidents likely to result in a risk to the rights and freedoms of data subjects
 |
| Caldicott Guardian | * Member of the Loss Panel
* Responsible for protecting data of adult service users who may be at risk.
* Consultee on whether a notification should be made to the ICO of any reportable incidents
 |
| Information Governance Solicitor | * Advisor to the Loss Panel
* Providing legal advice on the Data Protection Act 2018 including the GDPR
* Supporting the Data Protection Officer
 |

**Assessing risk and high risk**

Immediately upon becoming aware of a breach it is vitally important to

1. Contain the incident but also
2. Assess the risk that could result from it

Notification of a breach to the ICO is required unless it is unlikely to result in a risk to the rights of an individual. Notification of a breach to a data subject is required were it is likely to result in a high risk to the rights of an individual. This risk exists when the breach may lead to physical, material or non-material damage to the individual. Examples of such damage are discrimination, identity theft, fraud or financial loss and damage to reputation. Such damage is considered likely to occur when the breach involves personal data that reveals any of the following:

* racial or ethnic origin
* political opinion
* religion/philosophical beliefs
* trade union membership
* genetic/biometric data
* health
* sex life
* criminal convictions and offences
* data relating to security measures

When considering the risk to individuals as a result of a breach, the specific circumstances of the breach should be considered including the severity of the potential impact and the likelihood of this occurring. The following factors should be considered:

* Type of breach
* Nature (sensitivity plus volume of personal data)
* Ease of identification of individuals
* Severity of consequences for individuals
* Special characteristics of the individual
* The number of affected individuals
* Any other relevant factors

Further information about assessing the risk to individual is contained in the Data Protection Act 2018 and the GDPR and Article 29 Data Protection Working party Guidelines on Personal Data Breach Notification February 2018 <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.

**Record Keeping**

Regardless of whether or not a breach needs to be notified to the ICO, the Council is required to keep an internal register of breaches recording:

* Log number
* Details of the breach
* Cause of the breach
* What took place
* Personal data affect
* Whether or not the ICO is notified (with dates and reasons; was notification in phases, was it done within 72 hours, if not reasons for delay)
* Effect and consequences of breach
* Remedial or mitigating actions taken
* Was a Loss Panel convened, dates

Where this register contains personal information it will be retained in accordance with the provisions set out in the Council’s retention schedule.

**Process Maps**

### **Triaging an Incident**

N

Triage incident and discuss with Information manager

Is further information required?

Gather further information

Is the incident a Non-event?

Is the incident a Near Miss?

Incident is a confirmed Loss

1

2

3

Log incident details on the Data Breach Register and assign a reference number

IM Team notified of an Information Loss

Y

### **A Non-Event Incident**

1

Request confirmation from Information Manager and close incident

Update the Data Loss Register

Inform reporter and DPO of non-event status

### **A Near-Miss Incident**

2

Update Data Loss Register

IM team to arrange and attend meeting with:
Individual
Team Leader
IM Champion

Collect further information

Is further information required?

Complete Incident Investigation Report including Information Management comments

Have any recommendations been made?

Have all actions been completed?

Ensure all actions have been completed

Y

Y

N

Y

N

Close Incident

N

Update Data Loss Register

Inform reporter and DPO of outcome

###  **A Confirmed Loss**

3

Update Data Loss Register

IM team to arrange and attend meeting with:
Individual
Team Leader
IM Champion

Collect further information

Is further information required?

Complete Incident Investigation Report including Information Management comments

Information Manager to review Investigation Report and decide on further action

Y

N

Is Loss Panel to be convened?

Y

Convene Loss Panel. Invite:
CIO, DPO, IM, Caldicott Guardian, IM Champion, Head of service

Incident discussed at Loss Panel – Information to be handed back to the team

Is the incident going to be reported to the data subject

Service to report incident to the data subject

Have any recommendations been made?

N

N

Have all actions been completed?

Y

Decision made whether or not to inform ICO

CIO / DPO / Caldicott Guardian informed of incident

Ensure all actions have been completed

N

Y