Corporate Procedures

Information Security Incident Reporting

Date Created:	May 2018	
Version:	V1.0	
Location:	Governance	
Author (s) of Document:	Information Security Officer	
Approval Authority	Chief Officer - Governance	
Scheduled Review:	May 2019	
Changes:	February 2018	Procedure supersedes previous Information Security Incident Reporting Procedure, incorporates personal data breaches and complies with GDPR.

Information Matters

take your time and get it right

Information Security Incident Reporting

1. About this procedure

This procedure and associated templates set out the Council's process for reporting Information Security incidents and near misses.

This procedure supports the Council's information policies, and defines what a security incident is and how it should be reported.

2. What is an Information Security Incident?

An information security incident is the exposure of Council information to risk. This information can be in any format, including data and hardcopy, and stored in any system or on any device. The incident can be either a manual incident, such as loss or theft, or a cyber incident, such as a virus or hacking.

The following, non-exhaustive list gives some examples of information security incidents:

- Missing or misplaced documents (correspondence, case files, council reports, etc.)
- Overheard sensitive conversations
- Accidental or intentional password sharing
- Hacking
- Malicious software (malware) attacks (viruses, spyware, key-loggers, etc.)
- Lost, found or stolen information, media or mobile devices (laptops, phones, tablets, pen-drives, etc.)
- Unsecured, unattended information (unlocked cabinets or PCs, desks not cleared, etc.)
- Misuse of systems or information
- Unauthorised access to, or alteration, corruption or deletion of, data
- Sharing information with incorrect recipients
- Theft of or damage to data or systems
- Any personal data breach (i.e. any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data)
- Information Security breaches of the ICT Acceptable Use Policy

This list is not exhaustive and staff must ensure they report any incident where they have a reasonable belief that there is (or was) a risk to the security of information.

An information security near miss is an almost-incident, where there was no actual loss of information availability, confidentiality or integrity, but where there was the potential for serious, negative consequences. Such a loss was only prevented by fortunate events, not by pre-planned controls - this is why a near miss is sometimes called a 'close call' or a 'lucky escape'.

Physical security breaches, such as unauthorised access to buildings or secured areas, are subject to the Health & Safety Incident/Near Miss Reporting Procedure.

3. Why should Information Security Incidents be reported?

Information security incidents often have statutory or contractual reporting requirements. Without timely visibility of the incident through reporting, we may not be able to fulfil legal obligations. For example, failure to notify the Information Commissioner's Office about a personal data breach within 72 hours of any member of staff becoming aware of it may result in a fine of up to €10million. Additionally, the longer an incident goes unreported, the longer a vulnerability may remain unaddressed allowing the incident to escalate or for further incidents to occur.

Following this procedure, undertaking proper investigations and keeping adequate investigation documents will help ensure the Council's compliance with relevant legislation. Failure to investigate and document any incident in a timely manner may result in a fine of up to €10million.

It is important that near misses are also reported, as understanding information security weaknesses allows us to develop and implement systems and processes that are more robust, and which prevent near misses from becoming future incidents. This will protect our customers' individual rights and freedoms, as well as minimise damage to the Council's information assets and reputation.

4. Who is responsible for reporting Information Security Incidents?

This procedure applies to all staff, agency staff, elected members, contractors and sub-contractors, and to any person, without exception, who uses or requires access to Council information assets. We are all responsible for reporting information security incidents and near misses, and failure to do so may result in the Council taking any action that it considers necessary, including disciplinary action.

If any information security incident or near miss is reported to you by a customer or third party, this must also be reported in line with this procedure.

5. How do I report an Information Security Incident?

Only basic details are required to make the initial report, so as soon as you are aware of an information security incident or near miss, you should report it to your line manager and to the ICT Service Desk. The following information will allow the Service Desk to correctly route the call, if necessary, to an incident manager:

- Date of incident
- Place of incident
- Reporting Officer details
- Brief description of incident and details of the information affected (e.g. was it personal information? See Appendix 1 if you are unsure what this is)
- Brief description of the effects of the incident, such as systems and number of users or customers affected
- Brief description of any action taken once the incident was discovered

Do not include any further personal data about affected users or customers in this initial report within ServiceNow; you will be asked to provide that to the Incident Handling Team directly.

6. What happens after the initial report is made?

The nature of the information security incident reported will determine what happens next. The ICT Service Desk will make an initial assessment to determine the severity of the incident (see Appendix 2 for a breakdown of incident criticality levels).

A **no/low risk** incident will be managed within business as usual processes. Upon closure of the incident, your line manager will complete an investigation checklist (see Appendix 3) and email it, and any further documentation relating to the incident, to ISO@aberdeencity.gov.uk.

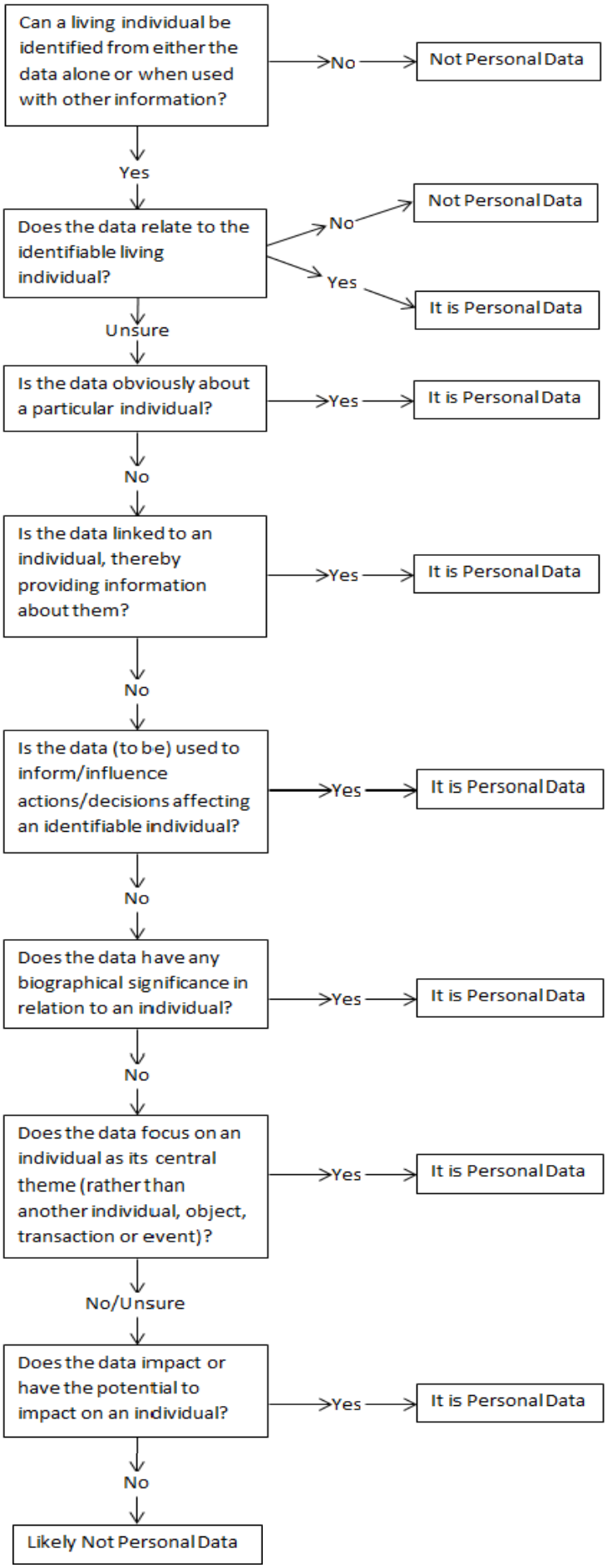
Medium and high risk incidents will be escalated to the appropriate team(s) for incident response. Depending on the nature of the information security incident, the teams involved in handling it will vary. However, each incident will have an Incident Handling Team Lead who will be responsible for coordinating the team's efforts in containing, investigating and remedying the incident. A variety of techniques and tools may be used by the Incident Handling Team to investigate an incident, and your cooperation with these is appreciated.

A workflow describing the investigation process for all incident types is available in Appendix 4.

7. Consequences of non-compliance with this procedure

Compliance with this procedure is mandatory and non-compliance must be reported to your line manager, who will determine the action to be taken. Any breach of this procedure may be treated as misconduct under the Managing Discipline Policy and Procedures.

APPENDIX 1: Workflow: Is this personal data?



Appendix 2: Incident Criticality

Risk Factor	No/Low	Medium	High
Defining Characteristics	Incident can be managed within normal operating procedures. No personal or sensitive information involved. Incident has minimal effect. Near Miss.	Sufficiently complex to require support of specialist teams. Service senior management needs to be notified. Personal data is/may/could be compromised. ICT Acceptable Use Policy breached.	A Major Incident affecting an information system. Serious breach of confidentiality or disclosure of sensitive personal data resulting in a high risk to the rights and freedoms of individuals. Any incident that requires involvement of law enforcement agencies or other external authorities.
Example Incidents	Encrypted laptop or other media device lost or stolen when switched off/locked. Unauthorised, accidental alteration of data through user error. Virus laptops/PCs with minimal effect. Hardware/software failure with minimal effect.	Encrypted laptop or other media device lost or stolen when unlocked. Unencrypted laptop or other media device containing confidential or personal data lost or stolen. Paper files containing sensitive or personal information lost. Email containing confidential or personal data being sent to an incorrect recipient. Personal data altered without permission.	Confidential or personal data incorrectly made publicly available on a website. Theft of customer database containing personal, financial information.

Please note: All incidents should be assessed on a case-by-case basis, and in light of the potential harm that could be done to an individual, a third party or Aberdeen City Council. This table is for guidance only.

Investigation background and Timeline

Date/ Time	Activity/ Event	Notified by
17/08/2025	Andy MacDonald received messages from SNP Partnership Leaders to advise that Councillor McLellan (an SNP Councillor) was erroneously listed as a Reform UK Councillor on the ACC website. Councillor McLellan had previously been listed as an SNP Councillor, which was correct.	Councillor Radley/Councillor Allard
17/08/2025 12:04	Jenni Lawson received a text from Andy Macdonald advising that Cllr McLellan was appearing as a member of Reform on the Council's website. Jenni contacted the Committee Lead who logged on and fixed the problem in Issue Manager and double checked that the website had been updated, which it had. The Chief Officer – Governance first messaged the Committee Lead on 17/8/25 at 12.33pm and the problem was fixed on 17/8/25 at 12.47pm.	Andy MacDonald
18/08/2025 08:34	Teams Message from Andy MacDonald to Jenni Lawson, Committee Lead, Steve Roud advising of error on Cllr McLellan's member page	Andy MacDonald
18/08/2025 08:57	Teams Message from Steve Roud to Service Manager Engineering & Operations asking him to stand up a security incident.	Steve Roud
18/08/2025 10:15am	In conjunction with our security, network, cloud engineering teams we analysed relevant access control and application log files to aid the investigation into the information change. It was confirmed from these that there was no evidence that suggests this was related to an unauthorised or cyber related change of the information contained within the system.	Service Manager Engineering & Operations
18/08/2025 10:30	Meeting with Security Team, Committee Services and vendor to initiate dialogue on probable causes.	Service Manager Engineering & Operations
18/08/2025 10:57am	Committee Services contacted the supplier to establish what happened.	Committee Clerk
18/08/2025 13:07	Teams message from Service Manager Engineering & Operations to Steve Roud advising that vendor are advising that likely cause is system software bug	Service Manager Engineering & Operations
18/08/2025 14:00	Meeting with Security Team, Committee Services and vendor confirms user behaviour and system bug as root cause. Vendor advised: "The bug occurs when you double click on a user, decide that you need to open a different record and then click 'switch records'. Depending on the network speed, timings, and Database load times, users may experience	Service Manager Engineering & Operations and Committee Clerk

	cross pollution between these records when editing the information from one record to the other and it has been found that the politics tab is quite prone to this issue occurring.”	

Appendix 3: Investigation Checklist

Check each box as the stage is completed. Delete/strikethrough options as appropriate. Once completed, email checklist and any associated documents to ISO@aberdeencity.gov.uk detailing the Incident's ServiceNow number.

ACTION

☐ Contain Threat
☒ Limit Damage
☒ Recover Losses

DETERMINE

☒	How did it happen? Incorrect information was published to an official Council page detailing information about elected members. The incorrect information has the potential to be embarrassing and politically damaging.		
	Source	Internal / ~~External~~	Internal threats have authorised access to systems/networks.
	Agent	~~Human~~ / ~~Environmental~~ / Technological	Human actors, such as users or hackers; environmental factors are natural; technological threats are problem hardware or software.
☒	Why did it happen? Vendor logs have confirmed that a staff member (acting within their assigned role) was updating Councillor McLellan's surgery information on Friday 15th August. These logs have confirmed that there were no updates being made to any Political affiliation to any elected member record. Findings from vendor have confirmed that this action has allowed the 'bug' to manifest without the user being aware. It appears that the incorrect information was displayed publicly from this date.		
	Intention	~~Deliberate~~ / Accidental	For Human agents only. If internal and deliberate, disciplinary proceedings are likely, cease investigation & contact HR and Legal.
	Was it malicious?	~~Yes~~ / No	Was harm intended? Environmental and technological agents are never malicious.
☒	What were the impacts? The incorrect information listed the Councillor as belonging to the Reform party. This created reputational damage and caused negative media interest		
	Information (refers to both data and information, in any format, on any device	☐ Destruction	
		☐ Corruption	
		☐ Theft	If internal, cease investigation & contact HR and Legal.
		☐ Loss	
		☒ Incorrect Disclosure	Disclosure of incorrect information to authorised recipients ie public web
		☐ Use Denial	
		☐ Privilege elevation	Granting/achieving access to information greater than that authorised

		☐ Illegal usage	If internal, cease investigation & contact HR and Legal.
	Service	☐ Loss	
		☐ Use Denial	
		☐ Privilege elevation	Granting/achieving access to information greater than that authorised

☒	How can we prevent it from happening again? 1. Amendment to standard operating procedures to ensure only single EM records are open at any time. Implement second check after any updates to provide independent validation that records are correct. 2. Issue Manager Build to be upgraded to the newest version at the earliest opportunity. Latest version will eliminate the known bug in the system software.

DOCUMENT

☒	What were the outcomes? Confirmation that vendor solution has a 'bug' that manifested when changing Councillor McLellan's surgery details. This was not visible to the user, and it is evident that no deliberate or malicious action has occurred from any employee. The actions below capture steps to avoid a reoccurrence.
☒	Any Actions?

Action	Owner	Completed On
Guidance to users on amended Standard Operating Procedure	Vikki Cuthbert	29/08/25
Confirm date of software upgrade	Vikki Cuthbert	

	What lessons have been learned? Knowledge of the bug in this software version was not known to Aberdeen City Council. We have asked that the provider to ensure that similar risks/bugs are shared with us in future.

Appendix 4: ISIRP Procedure Simple Workflow

INCIDENT OCCURS

1. Report incident to Line Manager

2. Report incident to ICT Service Desk

3. Initial Investigation & confirm facts

4. Check incident Risk Level against Criticality chart (see Appendix 2)

NO – LOW RISK

5. No further investigation required

6. Advise ISO that investigation is closed using Investigation Checklist (list any action taken, e.g. process improvements, actions to mitigate repeat occurrence, etc.)

Responsibilities

Notification Officer – actions 1 & 2
Line Manager – No-Low Risk, action 6
ICT Service Desk – actions 3 -5
Incident Handling Team Lead – Med-High Risk, actions 6-10

Action Owners

1 & 2 – Notification Officer
3-5 – ICT Service Desk

No-Low Risk, 6 – Line Manager
Med-High Risk, 6-10 – Incident Handling Team Lead

MEDIUM – HIGH RISK

5. Notify Incident Response Team, as per Information Security Incident Playbook

6. Incident Handling Team carry out full investigation. Notify and/or invite specialist teams to assist, as per the Playbook

7. ACTION: Implement any necessary continuity/containment plan

8. DETERMINE: If Investigation finds

- Illegal Activity
  - Cease Investigation
  - Notify Head of HR and Chief Officer – Governance who, together with ISO, will consider whether to notify Police Scotland (final decision to be taken by the Chief Officer – Governance)
- That disciplinary proceedings are likely
  - Cease Investigation
  - Notify Head of HR and Chief Officer - Governance who will decide on appropriate action, in line with the Disciplinary Process
- Another Government department is affected
  - ISO report incident to NCSC (National Cyber Security Centre)
- A Personal Data breach
  - Determine whether ICO (and affected individuals) need to be notified

9. DOCUMENT: Document & track Actions, Decisions, Evidence & Lessons Learned

10. Report incident, findings and outcomes to Information Governance Group