APPENDIX 9

Information Security Incident Reporting Procedure/Practice Note

May 2018

1. Introduction

1.1 Tameside Metropolitan Borough Council (the Council) will ensure that it reacts appropriately to any actual or suspected incidents relating to electronic or paper based information systems within the custody or control of the Council or its contractual third parties.

1.2 This procedure must be applied as soon as Council information or information systems are suspected to be, or are actually affected by an adverse event which is likely to lead to an Information Security Incident.

1.3 All incidents, irrespective of scale, must be reported using the incident management procedure to allow for lessons to be learned and to improve information handling procedures and the incident response process.

2. Definitions

2.1 The following terms are used throughout this document and are defined as follows;

Information Security Incident: is defined as an adverse event that has caused or has the potential to cause damage to the Council's assets, reputation, personnel and/or citizens.

An information security incident can occur when there is an actual or potential loss of information or when information is discovered (e.g. USB memory stick/paper files found or handed in).

On some occasions, an information security incident will include personal data and will entail a breach of the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR).

Examples of Information Security Incidents are provided at **Appendix 1.**

Personal information: is any personal data as defined by the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR). Broadly this is information about any living individual, who could be identified from the information or any other information that is in the possession of the Council. The Council is legally responsible for the storage, protection and use of personal information held by it as governed by the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR).

Special Category information: (similar to the concept of sensitive personal data under the Data Protection Act 1998). This data is covered by Articles 6 and 9 of the General Data Protection Regulations. As it is more sensitive it needs more protection and consists of:-

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health;
- sex life; or
- sexual orientation.

Protected Information is any information which is;

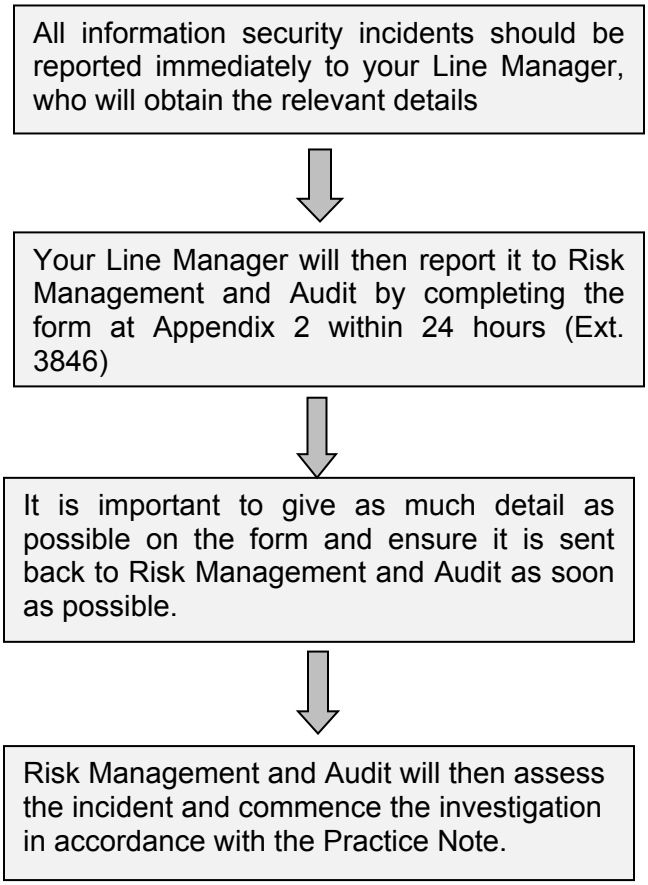
(a) personal/special category (sensitive personal data) or
(b) confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled manner.

3. Roles and Responsibilities

3.1 All employees must understand and adopt the use of this procedure and are responsible for the safe and secure use of Council information and systems.

3.2 All employees have a duty to report actual or suspected information security incidents and to fully support an investigation. Failure to report an Information Security Incident immediately or within 24 hours at the latest of discovery could result in disciplinary action.

4. Reporting an Incident



Note: If information has been discovered in any format (e.g. Memory Stick), it is important that you do not do anything with the information unless advised to do so by Risk Management and Audit. Report as you would normally through the information security incident procedure outlined above.

5. Incident Investigation

5.1 Initial Response

5.1.1 Once the Information Security Incident Form has been received an evaluation can take place to identify if, there may be a need for immediate action in order to limit the damage from the incident and recover any losses. Action may also be needed to prevent another incident with similar circumstances whilst the investigation is taking place. This may include action taken to:

- prevent any further unauthorised access;
- secure any affected buildings (i.e. changing locks, access codes etc.);
- recover any equipment or physical information;
- restore lost or damaged data by using backups; or
- prevent a further incident relating to the same information (e.g. an attempt to use stolen data to access accounts or services)

5.1.2 The Risk Management and Audit Team will determine if any immediate action needs to be taken based on the details provided and will notify the relevant persons.

5.2 Investigation Process

5.2.1 Risk Management and Audit at this stage will review the incident and consult with other information governance specialists in the Council where appropriate before an investigation will commence. The investigation may involve the following:-

- Senior Information Risk Owner (SIRO);
- Data Protection Officer/Data Controller;
- Service Director or a representative for the relevant part of the directorate;
- Line Manager of person who has caused the incident;
- Head of Human Resources or a representative;
- Head of ICT/ICT Security Officer;
- Head of Media, Marketing and Communications or a representative;
- Facilities Management; and
- Caldicott Guardian

5.2.2 Depending on the type and seriousness of the incident, the police may be involved and the employee/s suspended from the work place.

5.2.3 The Risk Management and Audit Team will use the checklist outlined at **Appendix 3** along with any other information required, to investigate the incident and will record any key findings from this point forward.

5.2.4 Once the investigation is completed, a summary of the incident will be presented to Senior Management for evaluation and signing off.

6. Evaluation

6.1 A consistent approach to dealing with all security incidents must be maintained across the Council and each incident must be evaluated. It is important not only to evaluate the causes of the incident but also the effectiveness of the response to it.

6.2 The evaluation of the information security incident will include some of the following questions:

- Had the incident been identified as a risk prior to its occurrence?
- Did the incident occur despite existing measures being in place?
- Were current policies and procedures followed? If not, why not?
- In what way did the current measures prove inadequate?
- How likely is the incident to recur?
- Did the incident involve deliberate or reckless behaviour?

6.3 Assessment of Ongoing Risk

6.3.1 Any identified weaknesses or vulnerabilities must be accurately assessed in order to mitigate the ongoing risks to information. In order to make an assessment, the following factors will be considered:

- Type of data involved;
- Number of people that could be affected;
- Impact on individuals;
- Protections in place (e.g. encryption);
- Likelihood of the identified risk;
- Possible consequences for the Council's reputation; and
- Potential risks to public health or safety.

7. Actions

7.1 Once the investigation and the evaluation of the incident is concluded, any identified actions will be approved by Senior Management and implemented appropriately throughout the Service involved or if required the whole organisation.

7.2 Notification

7.2.1 Depending on the incident there may be legal, contractual or sector specific requirements to notify various parties. Notification may assist in security improvements and implementation, as well as risk mitigation.

7.2.2 The following parties may need to be notified following an Information Security Incident:

- **Information Commissioner's Office (ICO)**
  - Does the incident involve personal data? If so:
  - Does the type and extent of the incident trigger notification?

  > We have to notify the ICO **within 72 Hours** of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.
- **Individuals**
  - Notification to the data subjects involved maybe required where the incident is likely to result in a high risk to their rights and freedoms.
- **Other Agencies**(not an exhaustive list)
  - Identity and Passport Service
  - Her Majesty's Revenue and Customs (HMRC)
  - Bank or credit card companies

- Trade Unions

7.2.3 Notification to any parties will be determined and agreed by Legal Services and Senior Management as part of the evaluation of an incident.

7.3 Disciplinary Action

7.3.1 It may be deemed necessary to follow the disciplinary procedure for any employee(s) involved in an information incident.

7.4 Policy and Procedural Changes

7.3.1 There may be a need to implement policy and procedural changes as a result of an Information Security Incident.

7.5 Employee Notification and Training

7.3.2 There may be a requirement to notify employees of policy and procedural changes and to repeat, extend or revise training following an Information Security Incident.

Appendix 1

Examples of Information Security Incidents

Examples of Information Security Incidents are listed below. It should be noted that this list is not exhaustive.

- Giving information to someone who should not have access to it - verbally, in writing or electronically
- Computer infected by a Virus or other malware
- Sending a sensitive e-mail to 'all staff' by mistake
- Receiving unsolicited mail of an offensive nature
- Receiving unsolicited mail which requires you to enter personal data
- Hacking attacks which intend to gain information from computers and/or systems using a number of methods (e.g. phishing, password cracking, key logging)
- Changes to information or data or system hardware, firmware, or software characteristics without appropriate authority or the Council's knowledge, instruction, or consent
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others
- 'Blagging' offences where information is obtained by deceiving the organisation that holds it (including information which could assist in gaining access to council data e.g. a password)
- Use of unapproved or unlicensed software on Council equipment
- Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password)
- Writing down your password and leaving it on display / somewhere easy to find
- Printing or copying confidential information and not storing it correctly or confidentially
- Theft / loss of a hard copy file
- Theft / loss of any Council computer equipment on which information is stored
- Discovery of hard copy information or electronic media on which information may be stored (e.g. disc or USB memory stick)
- Unwanted disruption or denial of service to a system which may cause an adverse effect to the information held within
- Equipment failure that results in the loss of or damage to information
- Unforeseen circumstances such as fire or flood that damages information or areas where information is stored
- Posting inappropriate comments or material online (including on social networks)

Appendix 2

Information Security Incident Reporting Form

Please send the completed form to the Head of Risk Management and Audit and DO NOT take any further action unless advised. The incident will be investigated and where appropriate a report issued for action.

Directorate/Service Area	
Assistant Director	
Service Unit Manager/Line Manager	
Employee Reporting Incident	
Person Responsible for Incident	
Date/Time of Incident	
Type of Data/Information Involved - (Paper/Email/Letter/Electronic Data)	

Details of Incident:	
Describe in detail how the incident has occurred?	
Did the employee self-report the incident?	
Are there any mitigating circumstances put forward by the employee?	
Outline what data/information is involved? e.g. • Health or Social Care? • Financial (e.g. bank details)? • Personally Identifiable Information (e.g. Name, Address, NI Number)? • Special category information (e.g. race, religion, health)	
Please attach a copy of the letter/document inadvertently disclosed.	
Approximately how many people have been affected?	
Is the incident a one off or has more than one incident occurred over a period of time? Please provide details and copies of letters etc.	
Has there been any media coverage of the incident?	
Are any other partners involved?	
Has the document/file/data/information been recovered?	
Immediate Action Taken:	
Have you taken any action to reduce the effect on the data subjects involved? If so please provide details:	

Signed: Date:

Job Title:

Return to: Head of Risk Management and Audit – Wendy Poole

Telephone: 0161 342 3846 **Email: wendy.poole@tameside.gov.uk**

Appendix 3

Information Security Incident Investigation Checklist

The following questions may be asked during the investigation process.

How was the incident discovered?

What type of data is involved?

- Health or Social Care?
- Financial (e.g. bank details)?
- Personally Identifiable Information (e.g. address, NI number)?

Whose data is involved?

- Service users, patients or customers?
- Councillors?
- Council employees?
- Suppliers or partners?

How many people could be affected by the incident?

What could the information be used for?

What impact has the incident on?

- **Data Subjects:**
  - Physical harm
  - Mental anguish/distress
  - Reputation/embarrassment
  - Financial loss
  - Identity theft
  - Breach/loss of confidence
- **Employees:**
  - Embarrassment
  - Mental anguish on employees involved
  - Interruption of service to clients
  - Loss of confidence in service provision
- **The Council:**
  - Embarrassment/reputational damage
  - Breach/loss of public confidence
  - Press involvement
  - Potential legal action

What immediate action has been taken to recover the information?

Had the incident been identified as a risk prior to its occurrence?

What controls were in place to prevent the incident?

How likely is the incident to occur again?

Are the relevant employees aware of current policies and procedures?

Did the incident involve deliberate or reckless behaviour by an employee?

Please note that this list is not exhaustive. Other questions may be asked depending on the nature of the incident.

Information Security Incident Reporting Procedure – Practice note

May 2018

Incident Reporting Procedure – Practice Note

This practice note is to be used in conjunction with the Incident Reporting Procedure.

1. Incident Reporting

1.1 All employees have a duty to report actual or suspected information incidents immediately.

1.2 Disciplinary action will be automatically invoked if an incident comes to light by way of a complaint or referral from the ICO where it had not been reported internally.

2. Initial Response

1.1 Once the Incident Reporting Form has been received by your manager it will be passed to Risk Management and Audit who will determine if:

- Any immediate action is needed in order to limit the damage from the incident and recover any losses.
- Any action is needed to prevent another incident with similar circumstances from occurring. This may include action taken to:
    - prevent any further unauthorised access
    - secure any affected buildings (i.e. changing locks, access codes etc.)
    - recover any equipment or physical information
    - restore lost or damaged data by using backups
    - prevent a further incident relating to the same information (e.g. an attempt to use stolen data to access accounts or services)
- The incident needs to be reported to the ICO.

2. Investigation Process

2.1 Risk Management and Audit will review the Incident Reporting Form in conjunction with People and Workforce Development and Legal Services (where appropriate) and based on the criteria below determine whether a formal investigation needs to be undertaken.

2.2 Assessment Criteria:

- Contained to less than 5 individuals
- First incident by employee
- Nature of information released
- Information recovered
- Limited impact on individual (E.G. No safeguarding issues)
- Any mitigating circumstances put forward
- Did the individual self-report the incident

2.3 If the answer is “Yes” to all the above criteria then an informal interview will be held with the employee to discuss the incident to determine if any corrective action is needed to processes and procedures or whether more training is needed. The disciplinary process will not be invoked. A memo will then be issued summarising the key points and circulated to:

- Data Protection Officer
- Director
- Assistant Executive Director

- Service Unit Manager
- Monitoring Officer
- Caldicott Guardian (Where appropriate)
- Senior Information Risk Owner (SIRO)
- Head of HR Operations and Workforce Strategy

2.4 A standard outcome letter will be sent to the employee (copied to manager) from Risk Management and Audit at the conclusion of the informal interview explaining that if any further incidents occur they may be subject to disciplinary action?

2.5 If the answer is "No" to any of the above criteria then a further assessment of the incident will be undertaken to determine if a formal investigation is required as part of the Council's Disciplinary Procedure. The list below details some further areas for consideration:

- Had the incident been identified as a risk prior to its occurrence?
- Did the incident occur despite existing measures being in place?
- Were current policies and procedures followed? If not, why not?
- In what way did the current measures prove inadequate?
- How likely is the incident to recur?
- Did the incident involve deliberate or reckless behaviour?
- Did the individual self-report the incident?

Appendix 3 in the Incident Reporting Procedure contains more questions for consideration.

2.6 If an incident is reported to the ICO then a formal investigation will be required.

2.7 The formal investigation will be conducted in conjunction with People and workforce Development and will follow the Council's Disciplinary Procedure. At the conclusion of the investigation Risk Management and Audit will issue a report which will be circulated to:

- Data Protection Officer
- Director
- Assistant Executive Director
- Service Unit Manager
- Monitoring Officer
- Caldicott Guardian (Where appropriate)
- Senior Information Risk Owner (SIRO)
- Head of HR Operations and Workforce Strategy

2.8 Depending on the type and seriousness of the incident, the police may be involved and the employee/s suspended from the work place.

2.9 Informing the data subject(s) involved will need to be determined on a case by case basis in conjunction with Legal Services.