The Linden Centre

Information Security Breach Policy

Signed by:		
	Headteacher	Date:
	Chair of Management Committee	Date

Last Updated	04th January 2021
Review Due:	04th January 2022

IB-20

Information Security Breach Procedure (v4.4)

1. Introduction

1.1 This procedure supports the Council's Corporate Information Security Policy (CISP) and **must be read in conjunction** with it. This procedure details the necessary steps to take if you have concerns that there has been a breach of personal identifiable information (PII – see 1.2 for examples) by Council officers, Members or third parties[1] contracted to provide Council services.

1.2 Some typical examples of PII include, but are not limited to:-

- **Personal Data –** e.g. name; address; telephone number; date of birth; NI number; bank account details
- **Sensitive/Special Category Personal Data –** e.g. information specifically relating to race and ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, biometric data identifying individuals, genetic data, health data, sexual preferences, sex life and/or sexual orientation

1.3 The principles of securing information (in accordance with Principle 6 of the Data Protection Act), can be found in the Council's Corporate Information Security Policy (CISP). For further guidance on information security contact Audit & Governance (part of Policy & Governance) on 01952 382537.

2. What is a possible breach of PII?

2.1 A breach of PII is where there has been a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, identifiable personal data.

There are many examples of what constitutes a possible data breach, typical examples are detailed below:

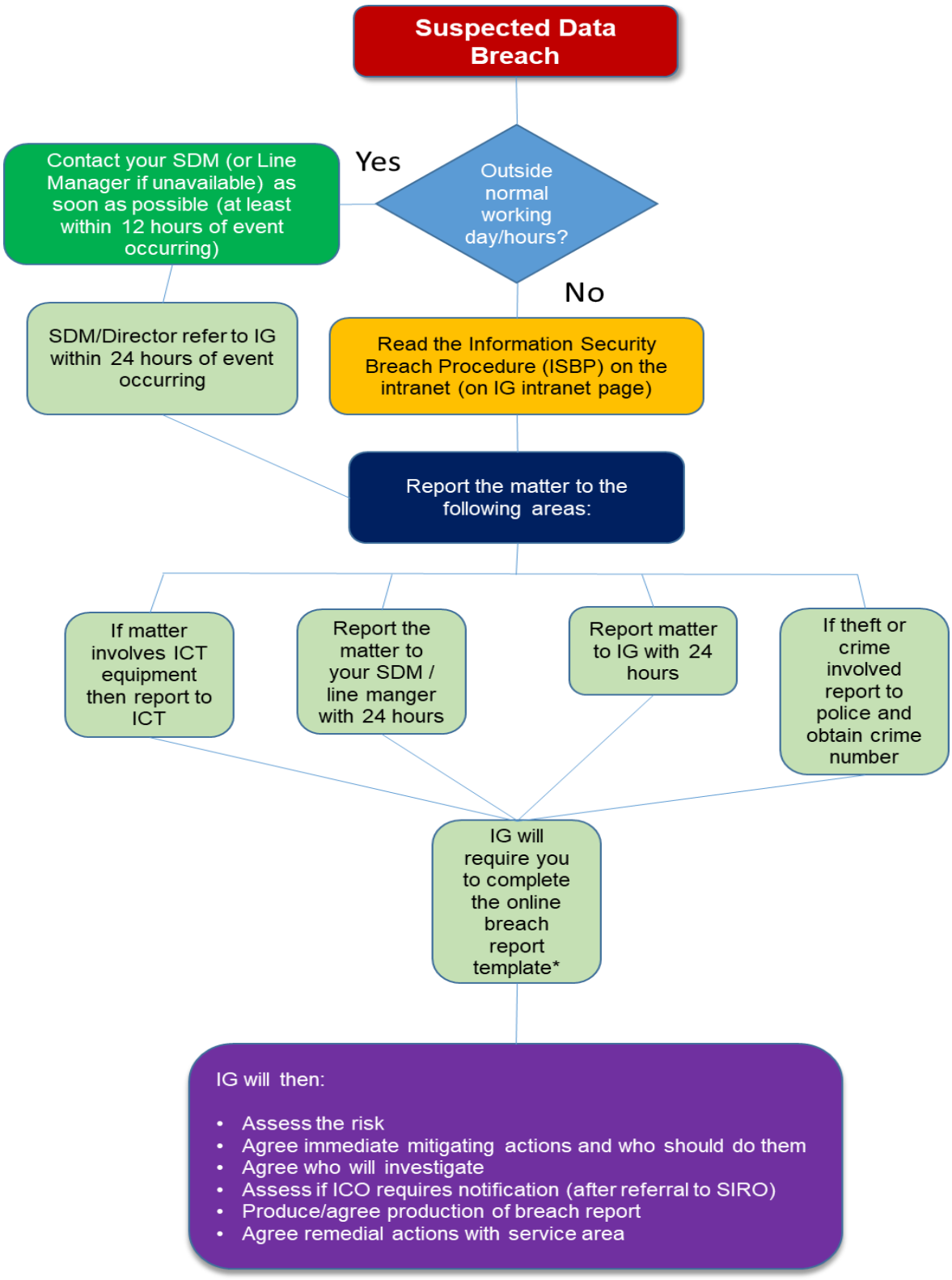
- Loss of mobile phone/laptop or other ICT equipment
- PII being emailed/posted/ to an unintended recipient or address and read by the individual, e.g. a letter containing social care information or financial information about an individual being sent to 36 Smith Street instead of 63 Smith Street (the intended recipient) and opened
- Loss of information/records relating to individuals and read by an unauthorised person, e.g. a lost file containing personal grant information
- Viewing PII that you do not need to access as part of your role
- Not keeping personal information secure; i.e. leaving correspondence on your desk at the end of the working day

2.2 There may be security incidents where PII has been given to an unauthorised person (due to a human or procedural error) but the recipient has not opened/read the PII. The PII has then been returned or it has been confirmed that it has been destroyed. Cases such as these should be

[1] Third parties could include temporary employees, agency workers, volunteers, partners or contracted service providers

notified to IG and the service area will be expected to undertake their own investigation into the security incident and implement actions that will minimise the possibility of a similar incident in the future.

3. What should I do if I become aware of a possible data breach?



*Online breach report template found on the IG intranet page

3.1 Outside a normal working day

3.1.1 If you become aware of a possible data breach you should report it immediately where you can. If this occurs outside normal working hours, e.g. bank holidays, weekends, etc., please contact your line manager within 24 hours of the incident occurring and then follow 3.2 below.

3.2 Normal working day

3.2.1 If you know/suspect a breach has occurred you will need to inform your line manager (who will inform the relevant Team Leader/Group Manager, SDM or Director) immediately (or as a minimum within 24 hours of incident occurring). The matter must then be forwarded to IG within 24 hours of the incident occurring for recording and investigation.

3.2.2 If the incident involves theft or a crime then you should contact the police and report this. Please make sure you obtain and record a crime reference number from the police where applicable.

3.2.3 If the incident involves the loss or theft of ICT equipment then this should also be logged with the ICT Service Desk on 83333 or via your desktop link.

3.2.4 When the matter is reported to IG and ICT (where relevant) the following information as a minimum should be to hand:

- Crime reference number given to you by the police (if applicable)
- Police station and constabulary the incident was reported to (if applicable)
- Place, time and date(s) the incident occurred
- Council officer and/or team(s) or 3rd party suppliers involved
- A summary of the information that has been lost, stolen or incorrectly communicated
- A list of the individuals affected or that could be at risk
- A list of organisations that may need to be contacted if applicable
- Confirmation as to who else in the authority has been informed, e.g. SDM, Director, Executive Director, Member, etc

3.2.5 When the incident is reported to the IG Team they will:

- Assess the level of the risk associated with the incident
- Agree the immediate mitigating actions that should take place and who should undertake them including who else needs to be informed (internally and externally)
- Agree who will undertake an investigation into the breach
- Compare the incident against notification rationale outlined by the Information Commissioners Office (ICO) and notify (after approval by the SIRO) if applicable
- Produce or agree the production of a breach report, see ***Appendix 1*** for required layout
- Agree remedial action to be taken by the relevant service area
- Communicate any lessons learnt corporately where appropriate

3.2.6 Managers can obtain guidance on possible action to be taken in relation to employees implicated in data breaches by accessing the relevant Human Resources guidance document on the intranet.

4. Advice and assistance

4.1 If you require any further information, or if you experience any difficulties accessing any documentation, please contact Audit & Governance on 01952 382537 or email IG@telford.gov.uk.

4.3 Alternative formats (i.e. hard copy, large print or Braille) of this procedure are available upon request.

Appendix 1

Suggested Report Template – ONLY TO BE USED IF ONLINE FORM UNAVAILABLE

(Input in grey below are example entries only)

Tick relevant box

Breach?	✓	Incident?	

See section 2 of this procedure for guidance on what constitutes a breach or incident

Date Occurred		Officer Implicated	*R Montgomery*

Date and name of SDM informed (and Director where relevant) *10/12/12/19 – Anthea Lowe*	Was breach/incident identified as a result of a customer complaint (Y or N?)	*Y*

Categories of Data Breached	Number of Individuals Affected	Number of Records Breached
Name, Address, Bank details	*1*	*6*

Description of breach/incident (including the type of information and date/location of incident)
Bank statements collected for identification purposes returned to 15 Darby Road on 10/12/19 instead of correct address 51 Darby Road

Reported to police Y/N?	*N*	Date Reported / Police Station	*N/A*	Crime number	*N/A*

Has information been returned to Council or destroyed?	Do you intend to notify the data subject(s) affected? If YES please consult IG prior to doing this If NO please give an explanation for this
Information returned to Council on 10/12/19	*Yes – as they will be able to ask their bank to watch their account*

How did breach/incident occur?
Officer had incorrectly updated the contact record for this customer

Measures already taken to address breach
1. Procedures for updating contact records reissued to all staff *2. Warning of this incident emailed to all staff* *3. QA checks to be put in place monitoring contact records accuracy*

Description of action (if any) taken against officer implicated in the breach/incident
Informal discussion with SDM and warning about future conduct

Lessons learnt to be implemented (if relevant)
1. Procedures for updating contact records reissued to all staff *2. Warning of this incident emailed to all staff* *3. QA checks to be put in place monitoring contact records accuracy*

Document Version Control

Version	Date	Author	Sent To	Comments
3.3	05/09/17	R Montgomery	Corporate - published	Final version
4	6/11/19	R Montgomery	Information Security Group	Requesting comments on updated text
4.1	14/11/19	R Montgomery	Governance & Legal SDM and SIRO	Version incorporates changes suggested by Information Security Group
4.3	11/12/19	R Montgomery	Publish	Includes further comments from ICT
4.4	7/2/20	R Montgomery	Governance & Legal SDM and SIRO	Version includes rebranding