**MADELEY TOWN COUNCIL**

**INFORMATION SECURITY BREACH POLICY**

**29 OCTOBER 2018**

# Introduction

1.1 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]](#footnote-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 Personal Data –** e.g.information specifically relating to physical or mental health or condition; race or ethnicity; political opinions; religious beliefs, or beliefs of a similar nature; membership of a trade union or non-membership;; sexual life; commission or alleged commission of an offence;

2. What is a possible breach of PII?

2.1 A breach of PII is where identifiable personal information has been or has the potential to be:

* Viewed or copied by an individual unauthorised to do so,
* Communicated to an unauthorised individual/organisation, e.g. sent to wrong address and opened/read
* Lost or stolen

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/faxed to an unintended recipient or address and read by the individual
* Loss of information/records relating to individuals and read by an unauthorised person, e.g. a lost file containing personal grant information
* Viewing PII on an ICT system that you do not need to access as part of your role
* Not keeping 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.

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

3.1 If a breach occurs or you suspect one has occurred you will need to inform your line manager within 12 hours of incident occurring. The matter must then be forwarded to Data Protection Officer within 24 hours of the incident occurring for recording and investigation.

3.2 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.

3.3 If the incident involves the loss or theft of ICT equipment then this should also be logged with Midlands Computers

3.4 When the matter is reported to the DPO 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 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 (e.g. shared service information), if applicable
* Confirmation as to who else in the authority has been informed

3.2.5 When the incident is reported to DPO 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 incident – low risk will be the council; medium – council/DPO by agreement; high risk – DPO.
* Compare the incident against notification rationale outlined by the Information Commissioners Office (ICO) and notify if applicable
* Produce or agree the production of an incident report, see ***Appendix 1*** for required layout
* Agree remedial action to be taken by the relevant service area
* Communicate any lessons learnt where appropriate

**Appendix 1**

**Suggested Report Template**

*Tick relevant box*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Breach?** |  |  | **Incident?** |  |

*See section 2 of ISBP for guidance on what constitutes a breach or incident*

|  |  |  |  |
| --- | --- | --- | --- |
| **Date Occurred** |  | **Officer Implicated** |  |

|  |  |  |
| --- | --- | --- |
| **Date and name of SDM informed (and the AD where relevant)**  *Informed Jenny Marriott* | **Was breach/incident identified as a result of a customer complaint (Y or N?)** |  |

|  |  |  |
| --- | --- | --- |
| **Categories of Data Breached** | **Number of Individuals Affected** | **Number of Records Breached** |
|  |  |  |

**Description of breach/incident (including the type of information and date/location of incident)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Reported to police Y/N? |  | Date Reported / Police Station |  | Crime number |  |

|  |  |
| --- | --- |
| 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 |
|  |  |

**How did breach/incident occur?**

**Measures already taken to address breach**

**BELOW SECTIONS TO BE COMPLETED ONCE INVESTIGATION ENDED**

**Description of action (if any) taken against officer implicated in the breach/incident**

**Lessons learnt to be implemented (if relevant)**

1. Third parties could include temporary employees, agency workers, volunteers, partners or contracted service providers [↑](#footnote-ref-1)