APPENDIX 1 –

PERSONAL DATA BREACH

1. What is a data breach?

The data protection legislation defines a personal data breach as "a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". For example, a data breach could be:

- Personal data being accessed by an unauthorised third party;
- Sending personal data to an incorrect recipient;
- Unencrypted electronic devices containing personal data being lost or stolen;
- Personal data being altered without permission; or
- Personal data being used for a purpose to which the consent was not given

2. Consequences of a personal data breach

A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property or social disadvantage. Therefore a breach, depending on the circumstances of the breach, can have a range of effects on individuals.

3. The Council's duty to report a breach

If the data breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported to the individual and ICO without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. The clerk of the Council must be informed immediately so they are able to report the breach to the ICO in the 72 hour timeframe.

If the ICO is not informed within 72 hours, the Council via the clerk must give reasons for the delay when they report the breach.

4. Notifying the ICO and the individual of a breach

When notifying the ICO of a breach, the Council must:

i. Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

ii. Communicate the name and contact details of the clerk;

iii. Describe the likely consequences of the breach;

iv. Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse affects.

APPENDIX 1 –

PERSONAL DATA BREACH

When notifying the individual affected by the breach, the Council must provide the individual with (ii)-(iv) above.

The Council would not need to communicate with an individual if the following applies:

- It has implemented appropriate technical and organisational measures (i.e.encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it;
- It has taken subsequent measures to ensure that the high risk to the rights and freedoms of individuals is no longer likely to materialise; or
- It would involve a disproportionate effort

However, the ICO must still be informed even if the above measures are in place.

5. The clerk's duty to inform the Council

If the clerk becomes aware of a personal data breach, it must notify the Council without undue delay. It is then the Council's responsibility to inform the ICO rather than the clerk's.

6. Records of data breaches

All data breaches must be recorded whether or not they are reported to individuals. This record will help to identify system failures and should be used as a way to improve the security of personal data. Data breaches will be recorded in the following format:

Date of breach	Type of breach	Number of individuals affected	Date reported to ICO/ individual	Actions to prevent breach recurring

To report a data breach, use the ICO online system at https://ico.org.uk/for-organisations/report-a-breach.