Appendix 6

West Dunbartonshire Council

(Information Security Policy Framework)
Reporting of Information Security Concerns

If anyone becomes aware of, or suspects that a violation of the Information Security Policy framework has occurred, whether from an internal or external source, paper or electronic records, they must comply with the guidance below.

Violations of the Information Security Policy may include, but are not limited to, any act that:

- Exposes the council to actual or potential monetary loss through the compromise of ICT security, eg clicking on a link within a phishing email;
- Involves the disclosure of confidential information or the unauthorised use of Council data, eg sending a letter to the wrong recipient, checking a neighbours balance;
- Involves the use of data for any illicit purposes, which may include violation of any law, regulation, or any reporting requirement of any law enforcement of government body;
- May result in the deliberate of inadvertent compromise of WDC systems or networks; and
- Contravenes the conditions laid in in the Councils Acceptable Use Policy.

This list is not exhaustive as the Information security landscape changes constantly, if in doubt, contact the ICT Security Officer and/or the Data Protection Officer.

Any individual who has knowledge of a violation of the Information Security Policy must report that violation immediately to one of the following

- ICT Security Officer;
- Data Protection Officer; and/or
- Line Manager.

If reported through the Line Management chain it is the Line Managers responsibility to ensure that the violation is brought to the attention of the ICT Security Officer and/or the Data Protection Officer.

Employees can also use the confidential whistleblowing process:
Whistleblowing - Employee Intranet