

Information Security Policy

Approved at Annual Council Meeting on 27th January 2020 (Minute 187/19/20)

Information security is the continuous process of exercising due care and diligence to protect information systems from unauthorised access, use, disclosure, destruction, modification, disruption, or distribution. It is an indispensable part of all the Council's business operations and requires ongoing training of both staff and councillors.

Security

- We will ensure that our paper and electronic systems are made secure against unauthorised access and disclosure of, or damage to, information and data; both by direct human access and indirect cyber-attack.

Assurance

- As part of our Disaster Recovery Plan, we will ensure that data are not lost when critical issues arise, as over time, there will be an inevitable exposure to one or more issues such as natural disaster, computer/server malfunction, physical theft, or malicious interference.
- Information kept solely in physical (paper) form that is critical to the operation of the Council e.g. deeds, contracts of employment, leases, will be copied and the copy held at a separate, trusted, location in secure storage.
- Information in digital format, which will increasingly be the majority of our information, will be regularly backed up and the backup drive stored in a separate, trusted, location in secure storage. All such back-ups will be encrypted and password protected.

Confidentiality

- We will protect the privacy of people's data and organisations on which we hold information, including commercially confidential information, by ensuring that our systems cannot disclose information to unauthorised individuals. (See also Data Protection Policy).

Integrity

- We will protect the integrity of our information by ensuring that data cannot be modified undetectably.
- For electronic systems, we will regularly review our anti-virus and firewall software to ensure that it remains fit for purpose.

Availability

- Information we need to run our business must be available when it is needed. We will ensure the proper functioning of computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it.

Authenticity

- We will, as far as possible, ensure that the data, transactions, communications and documents (electronic or physical) we retain are genuine.

