11 IT Infrastructure Security Policy

11.1 Scope

11.1.1 This policy applies to all users of the Council's owned or leased / hired computer facilities and equipment. The policy defines what paper and electronic information belonging to the Council should be protected and, offers guidance on how such protection can be achieved.

11.1.2 This policy should be applied whenever a user accesses Council information or computer equipment. This policy applies to all locations where information within the custody of the Council or information processing equipment is stored, including remote sites.

11.1.3 The purpose of this policy is to establish standards in regard to the physical and environmental security of the Council's information. The protection required needs to be appropriate to the level of information held and the consequential risks of unauthorised access.

11.1.4 This policy aims to mitigate the following risks:

- Unauthorised access to Council information.
- Unauthorised misuse or destruction of Council information.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of unauthorised access to PROTECT and RESTRICTED information.
- Potential legal action against the Council or individuals as a result of unauthorised access to PROTECT or RESTRICTED information.
- Council reputational damage as a result of unauthorised access to PROTECT or RESTRICTED information.

11.2 Applying the IT Infrastructure Security Policy

11.2.1 Secure Areas

11.2.1.1 Information Asset Owners **must** ensure PROTECT and RESTRICTED information is stored securely. A risk assessment should identify the appropriate level of protection to be implemented to secure the information being stored.

11.2.1.2 The Councils must ensure that their buildings have appropriate control mechanisms in place for the type of information and equipment that is stored there.

11.2.1.3 Access to secure areas **must** be adequately controlled and physical access to buildings should be restricted to authorised persons. Staff working in secure areas should challenge anyone not wearing a badge or equivalent identification tag. Each team **must** ensure that doors and windows are properly secured.

11.2.1.4 Identification and access tools/passes (e.g. badges, keys, entry codes etc.) **must** only be held by officers authorised to access those areas and should not be loaned/provided to anyone else.

11.2.1.5 Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge. An ICT Services employee **must** monitor all visitors accessing secure ICT areas at all times.

11.2.1.6 ICT Services will ensure keys to all secure areas housing ICT equipment are held securely and not stored near these secure areas.

11.2.1.7 Where an information security breach occurs, or a Council employee leaves outside normal termination circumstances, the employee's manager is responsible for ensuring that all identification and access tools/passes (e.g. badges, keys etc.) are recovered from the Council employee and arranging for any door/access codes to be changed immediately.

11.2.2 Non-Electronic Information Security

11.2.2.1 Information asset owners are responsible for ensuring all PROTECT or RESTRICTED information is stored securely. For example, using the controls

- Filing cabinets that are locked with the keys stored away from the cabinet.
- Locked safes.
- Stored in a Secure Area protected by access controls.

11.2.3 ICT Equipment Security

11.2.3.1 All general computer equipment **must** be located in suitable physical locations that:

- Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust and vibration.
- Limit the risk of theft – e.g. **if necessary** items such as laptops should be physically attached to the desk.
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people.

11.2.3.2 Users **must not** store Council information on the local hard drive of their desktop computer. Information should be stored on the Council's network where appropriate. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained. Users should refer to the Managing your Information guidance Note for guidance concerning network drives and the appropriate place to store Council information.

11.2.3.3 The ICT Technical Team will ensure all servers are sited in a physically secure environment. Business critical systems should be protected by an Un-interrupted Power Supply (UPS) to reduce the operating system and data corruption risk from power failures. The equipment **must not** be moved or modified by anyone without authorisation from the Head of ICT Services.

11.2.3.4 The ICT Support Team will record all items of ICT equipment on the ICT Services equipment inventory. The ICT Support Team will ensure the inventory is updated as soon as Council computer assets are received, moved or disposed of.

11.2.3.5 The ICT Support Team will ensure all Council ICT equipment is security marked and has a unique asset number allocated to it. This asset number will be recorded in the ICT Services equipment inventory.

11.2.3.7 The ICT Technical Team will ensure all network cabling is protected against interception or damage.

11.2.4 Equipment Maintenance

11.2.4.1 ICT Services and users **must** ensure that all of the Council's ICT equipment is maintained in accordance with the manufacturer's instructions and with any documented internal procedures to ensure it remains in working order. The ICT Service Desk will:

- Retain all copies of manufacturer's instructions.
- Identify recommended service intervals and specifications.
- Enable a call-out process in event of failure.
- Ensure only authorised technicians complete any work on the equipment.
- Record details of all remedial work carried out.
- Identify any insurance requirements.
- Record details of faults incurred and actions required.

11.2.4.2 The ICT Service Desk will maintain a service history record of equipment so that when equipment becomes older decisions can be made regarding the appropriate time for it to be replaced.

11.2.5 Security of Equipment Off Premises

11.2.5.1 Equipment taken away from Council premises is the responsibility of the user and should:

- Be logged in and out, where applicable.
- Not be left unattended.
- Concealed whilst transported.
- Not be left open to theft or damage whether in the office, during transit or at home.
- Where possible, be disguised (e.g. laptops should be carried in less formal bags).
- Be encrypted if carrying PROTECT or RESTRICTED information.
- Be password protected.

11.2.5.2 Users should ensure that they are aware of and follow the requirements of the Council's insurance policy for any Council ICT equipment taken off site. Any losses / damage to this equipment **must** be reported to the ICT Service Desk.

11.2.6 Secure Disposal or Re-use of ICT Equipment

11.2.6.1 Users must return any Council ICT equipment that is no longer required to the ICT Service Desk.

11.2.6.2 ICT Services will ensure any ICT equipment that is to be reused or disposed of has all of its data and software erased / destroyed. If the equipment is to be passed onto another organisation (e.g. returned under a leasing agreement) ICT Services **must** ensure the data removal is achieved by using professional data removing software tools.

11.2.6.3 ICT Services will ensure all software media is destroyed appropriately to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

11.2.7 Delivery and Receipt of ICT Equipment into the Council

11.2.7.1 In order to confirm accuracy and condition of deliveries and to prevent subsequent loss or theft of stored equipment, the following **must** be applied:

- ICT equipment deliveries **must** be signed for by an authorised individual using an auditable formal process. This process should confirm that the delivered items correspond fully to the list on the delivery note.
- The ICT Service Desk must be informed immediately of any receipt of ICT equipment and this should be collected without delay and the delivered items should be checked again against the delivery note.
- ICT Services will ensure all new ICT assets are recorded in the ICT equipment inventory.

11.2.8 Regular Audit

11.2.8.1 The Head of ICT Services will arrange for regular independent audits of the Council's information security arrangements and lead on any recommended information security improvements where necessary.