Information Security Policy Suite

Remote Working Policy

ISPS - 003

This policy is available in alternative formats upon request, such as large print or electronically. Please contact the Technology Services Management Team, to obtain a copy in a different format.

v

Approval Authority: {insert approval body here}

Approval Date: xx/xx/2019

1. Purpose

The purpose of this Remote Working Policy is to enable the Council to provide flexible working arrangements to its staff whilst maintaining the security of its information assets. This Policy is supplementing the Council's *Home Working Policy and Procedure*.

2. Scope

This policy applies to all staff, members, contractors and any other persons who have access to the Council's information, information systems and networks.

This policy applies to all information held, created, modified or accessed from the approval date of this policy. It includes information in any form, no matter whether it is stationary (i.e. at rest) or in transit.

It also covers the buildings, premises and systems which contain that information (see the Buildings, Infrastructure and Equipment Security Policy (ISPS-004)). This policy also covers the use of private residence if a member of staff is using their home as a designated workplace in agreement with their line manager.

3. Policy Statement

The policy of the Council is to ensure that it takes appropriate technical and organisational security measures that:

a. Enable staff to work remotely, including from home, according to business requirements and in agreement with their line manager.

b. Ensure, where the individual's home is designated as a fixed location from which to work, that the home has a suitable work space by undertaking a home-working self-assessment[1], repeating it on an annual basis as a minimum or if the individual moves home.

c. Provide secure remote access to the Council's information and systems to any staff authorised by their individual's line manager as necessary to perform their job function, see the Access Control Policy (ISPS-006).

d. Provide all staff working remotely with appropriate equipment and services to work according their work style, including from the home, e.g. encrypted laptop, printer, etc. See the Buildings, Infrastructure and Equipment Policy (ISPS-004).

e. Ensure any Council ICT equipment installed in a fixed remote location that needs to be moved to another location is performed by Technology Services staff

f. Ensure that all Council paperwork and equipment is retrieved from remote workers:

[1] These must include both DSE and Information Security Risk assessments and take account of any storage requirements in order to maintain the security of the Council's information.

f.1. where appropriate, before the individual leaves the Council's employment;

g. within one week of the remote working arrangement ending or as soon as is reasonably practicable; Provide appropriate insurance cover under the Council's Insurance policy for the damage to, loss or destruction of any Council Equipment that is under the guardianship of an authorised member of staff (excluding equipment in transit).

4. Responsibilities

As per the Information Governance and Security Policy (ISPS-001)

Additional responsibilities arising

Line Manager

The Line Manager shall be responsible, via their line management to:

a. Defining and authorising the remote working arrangements in accordance with the local Flexible Working policy and *Home Working Policy and Procedure*.

b. Ensuring that, where relevant, the self-assessment is carried out and any actions arising are addressed.

c. Retrieving any Council information or equipment that has been issued to a remote worker when the remote working arrangement or employment ends. NOTE: Any computer equipment must be returned to Technology Services.

4.1 Fixed Location Remote Workers (Designated and Occasional)

Their responsibilities include:

a. Ensuring that the confidentiality of all Council information is maintained and that it is handled in accordance with the Information Handling Policy (ISPS-009).

b. Ensuring that electronic information is secured on corporate systems up in accordance with the Backup and Recovery Policy (ISPS-007).

c. Ensuring that all Council equipment is handled in accordance with the Buildings, Infrastructure and Equipment Policy (ISPS-004).

d. Organising the return of computer equipment to Technology Services for the purposes of any support and maintenance that cannot be carried out remotely.

4.1.1 Personal and / or Sensitive Information

If you are required to take personal or sensitive information home you must:

a. Ensure that such information is stored in a lockable cabinet when not in use.

b. Ensure that the information is secure whilst on the move (i.e. in transit).

c. Ensure that information is not left in a vulnerable position where it may have accessed by unauthorised individuals (including family members).

d. Any personal and/or sensitive information used at home must brought back to the office to be securely shredded using the Council's authorised shredding facilities and / or services.

4.1.2 Council owned, managed or assured equipment

If council-owned, managed or assured equipment is installed in a fixed remote location, e.g. the employee's home, the member of staff will be required to sign the Confidentiality and Non-Disclosure Agreement Form acknowledging their individual responsibilities to ensure that:

a. Equipment provided by the Council is for use by the remote worker only and must not be made available for personal use by anyone else including other members of the employee's family or friends.

b. All reasonable care is taken to ensure that equipment is stored securely and kept out of view from the street.

c. Any material changes to security measures at their fixed location are brought to the Council's attention so that a review of the security arrangements or a further inspection can occur.

d. Equipment is not left in an unattended vehicle overnight. It must be secured in a vehicle's locked boot, where available, whilst on the move (i.e. in transit).

e. Equipment remains the property of the Council and use of it must be in accordance with the Information Security Policy Suite.

4.1.3 Personal equipment

See the Buildings, Infrastructure and Equipment Security Policy (004).

5. Training associated with this Policy

As per the Information Governance and Security Policy (ISPS-001)

6. Monitoring

As per the Information Governance and Security Policy (ISPS-001)

6.1 Non-compliance

As per the Information Governance and Security Policy (ISPS-001)

6.2 Review

As per the Information Governance and Security Policy (ISPS-001)

7. Equality Impact Assessment (EIA)

As per the Information Governance and Security Policy (ISPS-001)

8. Related documents

This policy should be read in conjunction with the following documents:

- ISPS-001 Information Governance and Security Policy;
- ISPS-004 Buildings, Infrastructure and Equipment Policy;
- ISPS-007 Backup and Recover Policy;
- ISPS-009 Information Handling Policy;
- Other policies in the Information Security Policy Suite;
- Any supporting standards, guidelines and procedures;
- The Council's Flexible Working Policy;
- The Council's Home Working Policy and Procedure.