Chelmsford City Council

Remote Working Policy

This is a transitional document to support the roll out of Office 365 which will enable remote working for eligible employees. The policy will remain under active review to ensure that it can facilitate the ICT Strategy for the Council.

INVESTORS IN PEOPLE | Gold

disability confident EMPLOYER

Chelmsford City Council

Contents

1 Introduction

Chelmsford City Council enables eligible employees to work remotely as appropriate and the purpose of this document is to state the Remote Working policy of the Council. The Council will ensure that all users who work remotely are aware of the acceptable use of portable computer devices and remote working opportunities.

2 Definition

Portable computing devices are defined as any electronic device that can be used in the creation, storage, and manipulation or transmission of council data.

3 Scope

This policy applies to all employees, elected members, contractors, agency workers, third party organisations or other authorised personnel who may remotely access the Council's Information Systems or information.

This policy applies to all employees who use Council IT equipment and personal IT equipment when working on official Council business away from Chelmsford City Council premises (i.e. working remotely) whether in the UK or abroad.

4 Roles and responsibilities

All roles and responsibilities are outlined in the Corporate Information Security Policy.

5 Management of Risks

5.1 The Council recognises that there are risks associated with users accessing and handling information to conduct official Council business.

This policy aims to mitigate the following risks:

i. Increased risk of equipment damage, loss or theft.
ii. Accidental or deliberate access to information by unauthorised individuals.
iii. Unauthorised introduction of malicious software and viruses.
iv. Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office or other legal action because of information loss or misuse and breach of Data Protection legislation.
v. Council reputational damage because of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

5.2 Data Protection

The Data Protection Act contains 8 principles that everyone responsible for using data must follow. All staff have a responsibility under the act to ensure that their activities comply with the Data Protection principles:

•personal data should be processed fairly and lawfully

•data should be obtained only for one or more specified and lawful purposes

•the data should be adequate, relevant and not excessive

•it should be accurate and where necessary kept up to date

•any data should not be kept for longer than necessary

•personal data should be processed in accordance with the individual's rights under the act

•data should be kept secure

•personal data should not be transferred outside the European Economic Areas unless the country offers adequate data protection.

Line managers have responsibility for the type of personal data they collect and how they use it. Staff should not disclose personal data outside the organisation's procedures, or use personal data held on others for their own purposes.

5.3 Employee responsibilities

It is the employee's responsibility to ensure the following:

5.3.1 Other Data security considerations

- Users must ensure security of portable computer devices when moving between home and another business sites.
- All employees will be responsible for securing any data accessed via Council systems is in accordance with data protection principles and ensuring that there is no unauthorised access to information
- Accessing emails or other data in a public place such as public transport can be allowed provided the users is sure that such access can remain confidential to the user
- To access Office 365 on a mobile device, you will be required to set a pincode as a second security step before you can access Office 365
- Office 365 will determine if there is sufficient virus protection on your personal device before it will download. If there is a security issue, you will not be allowed to download Office 365 to use remotely
- Hard copy information taken home as reference material should be securely stored in compliance with data protection principles and disposed of appropriately at the office base if the information is confidential or sensitive

- Any data breaches should be notified immediately to the line manager and the Information and Compliance Officer
- Confidential or sensitive information should only be emailed to a private non-Council email address following an approved request such as a subject access request for example.
- Information accessed through the Office 365 portal should not be downloaded to a personal device but saved to the Council system.
- When moving away from the computer or another mobile device, the screen should always be locked or the user should log off
- All users must be aware and comply with appropriate codes and policies associated with the use of IT equipment. This includes the following:
    - Corporate Information Security Policy
    - Conditions of Acceptable Use Policy
    - Removable Media Policy
- Any user accessing GCSx type services or facilities, or using GCSx protect or restricted information, must only use Council-owned equipment which has appropriate technical security

5.3.2 Agreement/arrangements to work at home

- The employee should notify their insurance and mortgage provider as appropriate that they occasionally work from home and should check that there is isn't anything that would prevent them working at home – for example in their mortgage agreement, lease or insurance
- Any requests for occasional remote working should be agreed in advance with the line manager
- Short notice requests to work at home or remotely may be agreed on a case by case basis
- Homeworking is not a substitute for suitable care arrangements and dependents need to be looked after by someone other than the employee when they are working and that, if necessary, care arrangements should be in place to cover the time when the employee is working
- While home working is a type of flexible working, employees should not assume that other aspects of flexible working (such as amended hours) are automatically part of a homeworking/remote working arrangement
- Variations to the usual working hours for the employee should be agreed in advance with the line manager
- The employee working at home must enable contact by office based staff as needed. This will involve the employee communicating clearly to their manager and colleagues when they are available and when they are not.
- The use of Skype for business status updates should be used to

indicate when the employee is available for contact

5.3.3 Health and Safety

- The work station used by the employee should be safe and should provide a secure and private space in which to work
- For occasional home workers, risk assessments of the work station should be undertaken by the employee and signed off by the manager before home working is allowed. For those whose main base of work is their home, the employer retains the responsibility for undertaking the necessary health and safety assessments

5.4 Manager responsibilities

It is the manager's responsibility to ensure the following:

5.4.1 Agreement/arrangements to work at home

- Should an employee be unwell it would not be expected that they will access any work accounts
- There is no requirement or expectation that employees on leave – annual leave, flexi leave or special leave – will access work accounts
- Some roles will be unsuitable for home working or remote working and the service manager will identify such roles and advise the employee
- Any request to work at home on a regular basis should be considered by the manager as a formal flexible working request and will be considered by reference to the Homeworking policy
- Agree outcomes for the employee working remotely and will monitor those outcomes to ensure productivity is achieved.
- In general, the employee should work the organisation's standard hours to meet business need but variations to working hours can be agreed by the manager on a case by case basis to meet operational need.
- Determine if the employee is suitable to work from home

5.4.2 Health and Safety

- Ensure that risk assessment documentation has been provided by occasional home workers and has been signed off by Service Managers.
- Should an employee have an adjustment to their office work station to enable safe working, this should be taken into account by managers when considering occasional home working requests
- The manager will ensure that risk assessments for dedicated home workers are undertaken by the Council and recorded appropriately

5.4.3 Expenses

- Whilst the manager may agree the issue of other resources such as paper for printing and printer cartridges it is expected that the employee should print hard copy documents, if needed, using office printing facilities
- No additional expenses such as for broadband or electricity will be paid by the Council for any employee who is an occasional home worker

6 Policy Compliance

If any user is found to have breached this policy, they may be subject to Chelmsford City Council's disciplinary procedure.

If you do not understand the implications of this policy or how it may apply to you, seek advice from HR or ICT Services as appropriate.

Appendix I - Council owned equipment

If issued with Council owned equipment users should not:

a. Install or update any software on to a Council owned portable computer device including screen savers

b. Save documents to any portable computer device hard drive

c. Change the configuration of any Council owned portable computer device.

d. Install any hardware to or inside any Council owned portable computer device, unless authorised by Chelmsford City Council's ICT Services (this includes portable storage devices).

e. ICT Services will deploy Anti-Virus software with the latest signature file to all Council IT equipment. Users will be responsible and expected to ensure Anti-Virus updates are occurring ensuring the device is up to date.

f. Users will inform the IT Service Desk of any Council owned portable computer device message relating to configuration changes.

g. All faults must be reported to the ICT Service Desk.

h. Users must not remove or deface any asset registration number.

i. User registration must be requested from ICT Services. Users must state which applications they require access to.

j. User requests for upgrades of hardware or software for Council IT equipment must be approved by a line manager through an ICT Service Request. Once approved the equipment and/or software will then be purchased and installed by ICT Services. Depending on the complexity of the upgrade the equipment may need to be returned to ICT in order the upgrade to be completed.

k. The IT equipment can be used for personal use by staff so long as it is not used in relation to an external business. Only software supplied and approved by Chelmsford City Council can be used (e.g. Word, Excel, Adobe, etc.).

l. No one other than the Council employee may use the Council supplied IT equipment. The IT equipment is supplied for the staff members' sole use.

m. The user must ensure that reasonable care is taken of the IT equipment supplied. Where any fault in the equipment has been caused by the user, in

breach of the above paragraphs, the Council may recover the costs of repair.

n. The user should seek permission from the Service Director before taking any Council supplied ICT equipment outside the United Kingdom. The equipment may not be covered by the Council's normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel.

o. The user should seek advice from ICT Services before accessing mobile services from outside the UK to be aware of the risks of using mobile technology abroad.

p. Chelmsford City Council may at any time, and without notice, request a software and hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.

Any IT equipment (including portable computer devices) supplied to users is the property of the Council. It must be returned upon the request of the Council. Access for ICT Services staff shall be given to allow essential maintenance security work or removal, upon request.

All IT equipment will be supplied and installed by ICT Service staff. Hardware and software must only be provided by the Council.

Where users access Government Connect Secure Extranet (GCSx) type services, facilities or RESTRICTED information, under no circumstances should non-Council owned equipment be used.

Version Number	Changes Made	Date of Changes
1	New ICT policy	1st March 2010
2	Amendments to support Office 365. Policy amended by HR and included in the HR framework of policies	May 2017