PART 5.5

INFORMATION SECURITY

CODE OF CONDUCT

Information Security Code of Conduct

It is very important that the council can ensure the security of information and systems used to store and process information. This document sets out the Information Security Code of Conduct (ISCC) for all members of staff as well as other system users as provided. This is supported by Corporate Information Security Policies which are available on the intranet. This Code of Conduct is also supplemented by a Supporting Manual which is available on the intranet. The ISCC is distributed to all relevant users.

All users will be required to confirm they have read and understood the Code of Conduct before ICT equipment is provided or access to systems, including the network, is granted. Breach of the Code could result in formal action, which may include disciplinary action in the case of employees, and withdrawal of access to all, or any of the Council's systems.

The ISCC and/or the underpinning policies will be amended as changes occur, for example to the ICT environment and/or wider information arrangements. Users will be advised in this event.

Information Security Code of Conduct

1. Who does this code apply to?

1.1 This document applies to anyone who uses, provides, or maintains Chelmsford City Council's (CCC) Information Technology systems. This includes staff (both permanent and temporary), contractors, agency staff, casual workers, work experience students as well as councillors. For easy reference, the term "users" will be used throughout this Code.

1.2 It applies to information (whether obtained from information systems or otherwise) that you hold at all times whether or not you are at work (staff and workers should also refer to the Council's "working flexibly – our approach" Policy). It does not apply to information relating to your private life or outside of work or to your use of your own or others IT systems.

1.3 Your use of any Chelmsford City Council's ICT facilities is subject to you reading, understanding, and formally agreeing to be bound by the terms and conditions of use set out in this document.

1.4 Breach of this Code may result in formal action, which may include disciplinary action, or withdrawal of access to some or all of the Council's systems.

2. Acceptable Use Policy

You must comply with the Council's Acceptable use policy. Users should not divulge any CCC information to third parties including forwarding or storing information in personal accounts unless it is appropriate or otherwise authorised for them to do so. By way of contrasting examples, it would not be appropriate for a staff member to forward Council work emails to any individuals outside of the Council, including friends or family. Whereas it would normally be reasonable for a councillor to share information provided to them in order that they can respond to a resident's inquiry, unless advised that the information is confidential or should not be released.

3. Cyber security & Malware

You must comply with the Council's Anti Malware policy.

4. Control over systems and data

4.1 You must not attempt to gain access to or manipulate any data for which you have no approval or need, to conduct your duties. You are responsible for understanding and adhering to your access rights to any given hardware, application system or data file.

4.2 Application systems and the ICT Infrastructure must not be changed unless formally authorised.

4.3 You must always save files relating to your CCC role to an appropriate location in accordance with the Council's Information Governance Policy and Information Storage Policy. Any transferral of data or information will be undertaken in accordance with the Council's Information Transfer Policy. Members or contractors may use non CCC IT systems and appropriate arrangements should be made in relation to the storage of any CCC information so that the information is kept secure.

5. Physical security

5.1 All users must be visibly identifiable as a council employee or as having authorisation to be on council premises, and where relevant, you must always wear your security badge and challenge those who are not wearing a badge.

5.2 You must not lend your access pass or personal keys to anyone.

5.3 Do not let anyone 'tailgate' you at any entrance unless they are wearing a valid CCC pass.

6. Printing

Use of CCC printing resources (printers, ink, paper) for personal or otherwise non CCC business reasons must be kept to an absolute minimum, especially colour printing. As a general guide, occasional printing of no more than one or two pages may be printed for personal use but anything additional to this should be specifically authorised by an appropriate manager.

7. Flexible Working

Staff must comply with the Council's "Working flexibly – our approach" Policy.

8. Confidential waste

You must comply with the Council's Disposal of Information Policy.

9. Legal requirements

All users must comply with the following legislation in their work:

Data Protection Act 2018
Freedom of Information Act 2000
Computer Misuse Act 1990
Health and Safety Act 1974
Copyright Designs and Patents Act 1998
Regulation of Investigatory Powers Act 2000 (as amended)

Most council procedures and systems are structured to ensure compliance with this legislation, but if you have any concerns or queries you should raise them with an appropriate manager or staff in legal services.