Chelmsford City Council Governance Committee

17 January 2024

Proposed Changes to the Constitution

Report by:
Monitoring Officer

Officer Contact:
Lorraine Browne, Legal & Democratic Services Manager & Monitoring Officer,
email: lorraine.browne@chelmsford.gov.uk, tel: 01245 606560

Purpose

To consider and/or note proposed changes to the constitution. and to note two other minor changes to the constitutional documents.

Recommendations

1. To consider a proposal to change to the terms of reference for the Treasury Management and Investment Sub Committee to increase membership from 5 to 7 councillors.
2. To note two other minor changes to the constitution. Firstly, changes to the Information Security Code of Conduct and secondly the Employee Code of Conduct.

1. Terms of reference for Treasury Management and Investment Sub Committee

1.1. The current terms of reference make provision for 5 councillors to sit on this committee. It is proposed to increase membership to 7 councillors.

1.2. This is a politically balanced committee, and the proposal has arisen to enable a councillor from the Independent Group to sit on this committee. A further administration member will also be added to the committee.

2. Other proposals for noting:

2.1. The Information Security Code of Conduct is being updated under officer delegation to reflect current working practices and to align with existing digital and HR policies. For noting is that both councillors and contractors are being added to the list of parties that are bound by the Information Security requirements.

2.2. The guidance manual which is currently within the Information Security Code of Conduct is also being separated and will become a Constitutional Practice Note. This will make it easier to communicate the requirements of the Information Security Code of Conduct which are now much shorter. The final draft version of the Information Security Code of Conduct can be found at Appendix 1 to this report.

2.3. The Monitoring Officer will be consulting the Chair of Governance Committee as to the application of the code to councillors and the content of the code of conduct and guidance manual/constitutional practice note in this regard.

2.4. A clarification to the appendix to the Employee Code of Conduct which is the register of interest form for employees. The form conflicts with the policy as to who approved a second employment for an employee. The update will clarify that the relevant “Line Manager” makes this decision as opposed to a director.

List of Appendices:

Appendix 1 - Part 5.5 of Constitution, Information Security Code of Conduct

Background papers: Nil

Corporate Implications:

Legal/Constitutional: These are set out in the report.

Financial: None

Potential impact on climate change and the environment: None

Contribution toward achieving a net zero carbon position by 2030: None

Personnel: None

Risk Management: None

Equality and Diversity: None

Health and Safety: None

Digital: None

Other: None

Consultees: Constitutional Working Group

Relevant Policies and Strategies:

Digital/HR policies referred to in Information Security Code of Conduct, Member Code of Conduct & Operational Manual supporting the Information Security Code of Conduct (updating of the Operational Manual pending)

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 to the ICT environment and information systems occur. 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 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 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.

1.3 Breach of this Code will 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. In addition to the requirement within this policy that emails should not be forwarded to personal email accounts, it should also be noted that the contents of emails should not be divulged to any individuals outside of the organisation, including friends or family.

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 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.

5. Physical security

5.1 You 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

Printing for personal 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.