Nottinghamshire County Council

Email Retention Standard

At a glance …

- Emails must be managed like any other record, and in keeping with relevant information legislation including the Data Protection Act 2018 and Freedom of Information Act 2000.
- Any email which is deemed a record must be saved to the relevant business system.
- Emails should not be retained for longer than is necessary.
- Over retention of emails gives rise to risks pertaining to regulatory compliance, data security, system performance and cost.
- The County Council will have in place controls to ensure emails cannot be retained longer than a defined period of time, which will be communicated to staff and affected users.
- The prescribed retention periods will vary depending on the assigned status of each individual email (i.e. whether it is sent, received, junk or deleted).
- By exception, the County Council will have in place a dispensation form to enable certain staff members to claim an exemption, where this is necessary, proportionate and justified against a clear business reason(s).
- Requests for dispensation must be approved by the Information Governance team and applied by ICT subsequently.
- Email accounts (including their content) assigned to employees that have left the organisation will only be retained for a short period of time beyond their exit date.
- Requests for emails by people asking for their own data (i.e. a Subject Access Request) or as part of Freedom of Information request will be referred to the Complaints and Information Team, or HR where it relates to employees or former employees.

Introduction

1. The County Council uses emails as a vital part of its daily work to conduct its day-to-day business activities. Email can be used to confirm agreements, approve business transactions, to share information and to gather information.

2. Emails that contain information which identifies living individuals are subject to the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018. Otherwise they may be subject to the Freedom of Information Act 2000.

3. Under data protection law, personal data should not be retained longer than is necessary. This applies to personal data contained in emails; however, emails themselves do not inherently have a defined retention period, rather the retention period should be determined by the purpose and content of individual emails.

4. The County Council recognises that the risks associated with uncontrolled email growth include the following:

    a. **Regulatory compliance** - retaining data beyond what is necessary is contrary to data protection and records management principles and increases the burden of responding to information rights requests under Data Protection and Freedom of Information (FOI) legislation (i.e. Subject Access and FOI requests)

    b. **Security risks** - storing excessive emails can expose the organisation to security threats and data breaches, the latter carries more severe penalties if over-retained data is breached

    c. **Performance issues** - large mailboxes can slow down email clients, affecting productivity.

    d. **Cost implications**: Managing large volumes of emails can incur additional costs for backup, security, and data migration.

Purpose of this document

5. The purpose of this document is to set out the standards that the County Council will implement to enable effective and proportionate email retention control and set out the expectations of its staff in managing emails effectively by ensuring they are retained for the correct length of time.

6. In doing so, the document will outline the County Council's approach to managing email retention in a way which meets data protection and records management principles in a pragmatic and proportionate manner.

7. It forms part of the County Council's Information Governance Framework and sits under the Information Compliance Policy.

Scope

8. The principles and commitments set out in this procedure apply to all employees, trainees / apprentices and volunteers of the County Council and to contractors, suppliers and partners delivering County Council services on our behalf.

9. Members of the County Council are not currently subject to this Standard, however they should note that they are also data controllers in their own right and are therefore responsible for ensuring any personal information they hold/use in their constituency role is managed in accordance with the relevant legislation.

Definitions

10. An email is defined as electronic mail, including attachments, that is sent by an email system or by text message on a mobile device.

11. A record is defined as '*information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.*'[1]

12. This definition applies to all records, in any format, irrespective of the medium it is stored (i.e. records can be paper or electronic, photographic or video images, audio recordings etc).

Principles & Commitments

13. The County Council has a legal duty to properly manage the records it holds. This includes all emails that fall within the definition of a record.

14. Email records should not be held longer than is necessary for the purposes that they relate to.

15. All staff are responsible for managing their emails and storing them in a way that ensures they can be identified and retrieved when required. Where an email is considered a business record and is required to be retained, it should be removed from an individual's inbox and placed within the relevant records repository such as Mosaic, SharePoint etc where it will be subject to the defined retention rules of that system (where such retention rules exist and are enabled).

16. The County Council will have in place controls to ensure emails are automatically deleted from MS Exchange (Outlook email client) after a defined period of time determined by relevant trigger events such as when the email was initially received or when a staff member has left the employment of the County Council.

17. Dispensations for individual staff members will be considered on a case-by-case basis and only granted where it is evidenced that there is a strong rationale to be exempt from corporate retention controls applied to email.

18. Where an individual staff member seeks to be exempt from corporate retention rules applied within their email client, they should submit the email retention dispensation request form (at appendix A) to the Information Governance Team.

19. The Information Governance team will consider the request and take into account factors including but not limited to; the seniority of the staff member, whether the staff member holds a statutory role and / or any other substantive reason.

[1] As defined in the ICO's Section 46 Code of Practice – records management

20. Where a dispensation is approved, the relevant retention rules set out in this Standard will not apply by default, however this does not exempt the staff member from continuing to manage their email account appropriately in keeping with the wider principles herein.

21. ICT is responsible for applying any approved dispensation for individual users on the instruction of the Information Governance team. The Information Governance team will maintain a record of agreed and rejected dispensations.

22. Approved dispensations may continue to be monitored by ICT and Information Governance to ensure they remain valid.

23. All data, information and records (regardless of the media in which they are stored) must be retained for the period of time identified in the Council's Records Retention and Disposal Schedule.

Email retention

24. Emails will automatically be deleted from inboxes and certain folders after a defined period time in keeping with the corporate records retention and disposal schedule and the County Council's limited number of corporate retention periods in use.

25. Deleted items and items stored in the "junk" folder will also automatically be deleted on a regularised rolling basis. In the event such items are considered records and consequently need to be retained, users should move them to alternative repositories as appropriate.

26. The length of time emails will be retained before being automatically deleted is set out as follows:

Email type	Retention trigger event	Automatically delete at
Emails held in inbox and all sub folders	Date of receipt	7 years
Emails sent out (sent items)	Date email sent	7 years
Junk items (where they remain in junk folder)	Date of receipt	30 days
Deleted items	Date email moved to deleted items folder	30 days
Email account (leavers)	Date employment terminates	90 days as per standard leavers process timescales

Responsibilities

27. Individual staff are responsible for managing their own email records by identifying and retaining email records and saving or uploading them into the relevant business systems.

28. Duties assigned to specific roles referenced in this procedure must be carried out as described below. The County Council's Information Governance Framework

provides further detail of the nature of specific information governance related roles (e.g. that of SIRO, Caldicott Guardian, Data Protection Officer etc.), see also the intranet page on IG roles and responsibilities.

29. The Information Governance team in conjunction with ICT will ensure guidance and awareness of the principles of this Standard are in place and communicated to the organisation as appropriate.

30. Requests for emails by people asking for their own data (i.e. a Subject Access Request) or as part of Freedom of Information request will be referred to the Complaints and Information Team, or HR where it relates to employees or former employees.

Compliance with this Standard

31. Wilful or negligent disregard for information governance policies, procedures and standards will be investigated and may be treated as a disciplinary matter under the relevant employment procedure(s) which could lead to dismissal or the termination of work agreement or service contracts.

Review

32. This Standard will be regularly monitored and reviewed by the Data Protection Officer (or their nominee) who will revise it in accordance with any learning arising from its implementation.

33. Beyond that, the Standard will be monitored and reviewed every three years taking into account legislation and codes of good practice.

Related legislation

34. Related legislation includes:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2000

Related Council policies/strategies/frameworks/programmes, partnership agreements etc.

35. Related Council policies/strategies/frameworks/programmes, partnership agreements include:

- Information Governance Framework
- Information Compliance Policy
- Information Rights Policy
- Information Security Policy
- Acceptable Use Standard
- Encryption Standard
- Information Security Classification Standard
- Password Standard
- Records retention and disposals schedule

- Data Destruction Standard
- Subject Access Requests Procedure
- Data Subject Right Procedure

Advice, Support & Further Information

36. Further advice about this Standard can be obtained from:

Information Governance Team Email: data.protection@nottscc.gov.uk Telephone: 0115 80 43800	**ICT Service desk** Email: itservicedesk@nottscc.gov.uk Telephone: 0115 97 72010:

37. Further reading and supporting information:

Title (as hypertext link) and publication date	**Author**
Section 46 Code of Practice – records management	Information Commissioner's Office

Document Control

Owner	Data Protection Officer
Original Author	Jason Monks
Last Reviewer	Jason Monks, Data Protection Officer
Approver	Information Governance and Cyber Security Board
Date of Approval	05/02/2025
Date of next review	05/02/2028
Version	1.0
Classification	Public

Version	**Date**	**Changes and Approver**
1.0	05/02/2025	Approved by IGCSB
1.1	16/05/2025	Minor amends to clarify IGCSB position on retention of email held in inbox subfolders.