

Cabinet

Date of Meeting: 04 December 2018

Report Title: Notice of Motion - Email Retention

Portfolio Holder: Councillor Paul Bates / Councillor Paul Findlow

Senior Officer: Mark Taylor, Interim Executive Director of Corporate Services

1. Report Summary

- 1.1. The purpose of this report is to consider and respond to the following motion which had been moved by Councillor Dorothy Flude and seconded by Councillor Suzanne Brookfield and referred to Cabinet for consideration at the Council meeting 18th October 2018:

“Recognising the implications of both GDPR and Freedom of Information Act legislation, this Council defers any changes to the policy the retention of emails until all police investigations, Crown Prosecution decisions and possible court actions are complete.”

- 1.2. Since the notice of motion, further briefings have taken place with portfolio holders Councillor Bates and Councillor Findlow, the Corporate Leadership Team, Information Governance Team and the Data Protection Officer to ratify that the email retention policy is compliant, fit for purpose and in accordance with legislation. All consulted parties have endorsed and approved the policy.
- 1.3. Objective 6 of the Corporate Plan states that Cheshire East is a responsible, effective and efficient organisation. Adoption of a compliant email retention policy aligns to this objective and supports organisational compliance and responsible management of information.

2. Recommendation/s

That Cabinet

- 2.1. Endorse the implementation of the email retention policy.

- 2.2. Agree that the policy will be technically enabled to the groups identified as in scope this financial year, with the view of implementing the policy across the whole organisation, where appropriate, by April 2020.

3. Reasons for Recommendation/s

- 3.1. GDPR directs that personal, sensitive data must not be retained for longer than is necessary. Wholesale retention of emails which may contain personal or sensitive data may therefore result in a breach of the GDPR.
- 3.2. The email retention policy does not mandate wholesale deletion of emails; it is to ensure the organisation treats email as a business record where applicable and to store it with the right retention, controls and measures against the right case file.
- 3.3. Organisational decisions, case related information, supporting papers and corporate records must be kept outside of email accounts.
- 3.4. Information must be stored in the correct location or system to preserve its integrity and prevent unintentional or deliberate loss.
- 3.5. The email retention policy will enable the organisation to have greater control over its information with regards to audit, retention, deletion.

4. Other Options Considered

- 4.1. The current state and management of email information is an area which lacks compliance and governance controls and therefore there are no other known options to consider.

5. Background

- 5.1. The email retention policy will mandate that email retention of two years will be applied to officer accounts and retention of six years to member accounts. The policy will mandate technical automation of the policy across the email system.
- 5.2. All accounts will qualify for litigation hold meaning all emails will be kept for 2 years regardless of whether the user has deleted it from Outlook. Therefore, all email under litigation hold will be available for review if required in the future.
- 5.3. Implementation of the email retention policy will be phased and there will be a robust process for exemptions. First phase deployment of the policy which is planned for this financial year will exclude:
 - 5.3.1. Members
 - 5.3.2. Corporate Leadership Team

- 5.3.3. Childrens and Families Service until the Independent Inquiry into Child Sexual Abuse (IICSA) concludes or new guidance received
 - 5.3.4. Email accounts pertaining to on-going investigations
 - 5.3.5. Email accounts of those away due to long term absence
 - 5.3.6. Shared Services
- 5.4. The above exemptions account for 21% of the organisation. First phase policy implementation will be applied to 79% of the organisation.
 - 5.5. For the 79%, all emails prior to May 2017 will be archived in the Enterprise Vault irrespective of deletions of these emails in Outlook. ICT can recover these items for a period unless they have been deleted by the Officer prior to archive; therefore there is no additional risk of data loss.
 - 5.6. Emails are currently being stored with no deletion or management of information and there is a lack of corporate control. There is a risk that information could be lost either through inadvertent or deliberate deletion.
 - 5.7. Email systems do not provide the same controls as case or content management systems. The email system is designed to be a transitory communication tool. Storing information in a case or content management system means information can be stored with the correct controls in place.
 - 5.8. The email retention policy does not jeopardise the availability of information, or weaken governance controls.
 - 5.9. The risk of manipulation or security of information is higher in Outlook as it does not have the controls to manage information compliantly. Once information is in a case management system it will be more secure as most case management systems prevent user destruction of information, and have in-built audit trails in terms of who is accessing, amending and deleting records.
 - 5.10. Email information must be managed, kept securely, stored as justified, kept confidential and retained only for the correct period of time as this is central to compliance (Computer Misuse Act, the Freedom of Information Act (FOIA), GDPR, Data Protection Act 2018 and the Public Records Act).
 - 5.11. Information kept beyond the correct retention periods will contravene compliance. GDPR clearly outlines and directs that information should only be kept for as long as it is needed for the business need. Article 5 of the GDPR directs that this must be adopted as a principle.
 - 5.12. Records beyond retention should not be kept for the purposes of Freedom of Information (FOI) and it is not a requirement of FOI to keep information indefinitely.

- 5.13. The ICO's Code of Practice published under Section 46 of Freedom of Information Act (FOIA), provides recommended good practice to public authorities in relation to keeping, management and destruction of their records. The email retention policy aligns to best practice and compliant working.
- 5.14. The Information Assurance, Data Management and Governance team have evaluated the risk associated to policy implementation and have ensured mitigations are in place to negate any concerns regarding information loss. It is noted that this is a significant change to the organisation, but a vital step in leading the organisation to a state where information is managed compliantly.

6. Implications of the Recommendations

6.1. Legal Implications

- 6.1.1. Compliance with GDPR and UK data protection legislation is mandatory; penalties for the Council as a Data Controller under GDPR can now be up to €20 million (£17m).
- 6.1.2. GDPR directs that personal data must not be retained for longer than is necessary. Wholesale retention of emails which may contain personal data may therefore result in breach of the GDPR.
- 6.1.3. FOIA amends the Public Records Act 1958 and places obligations on public authorities to maintain their records in line with the provisions of a code of practice on records management issued by the Secretary of State under Section 46 of FOIA. Failure to comply with the code is not in itself a breach of FOIA or the EIR. However, following the code will help the organisation comply with the legislation.
- 6.1.4. While all email accounts will qualify for Litigation Hold and kept for 2 years, consideration should be given to the limitation periods applicable in England, currently 6 years for simple contracts and certain actions in tort and 12 years in relation to deeds. Litigation may therefore be commenced at any time up to 6 years following breach of contract simple contracts and the cause of actions in tort or 12 years in respect of deeds. Storage of emails in case or content management systems will either need to be embedded in the processes of services or enabled automatically to ensure compliant management of records and access for the purpose of litigation.

6.2. Finance Implications

- 6.2.1. Compliance with GDPR and UK data protection legislation is mandatory; penalties for the Council as a Data Controller under GDPR can now be up to €20 million (£17m).

6.3. Policy Implications

6.3.1. This supports Objective 6 in the Corporate Plan.

6.3.2. Revisions of the ICT Email and Messaging Policy will be made to reflect email retention.

6.4. Equality Implications

6.4.1. None.

6.5. Human Resources Implications

6.5.1. Under the new GDPR data subjects can obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. This requirement cannot be met if email is used as a storage mechanism for information.

6.6. Risk Management Implications

6.6.1. None.

6.7. Rural Communities Implications

6.7.1. None.

6.8. Implications for Children & Young People

6.8.1. The Childrens and Families Service will be exempt from the automation of the email retention policy until the Independent Inquiry into Child Sexual Abuse (IICSA) concludes or new guidance received. However the Service will still be briefed on the compliant practice of not storing corporate records or case information in Outlook.

6.9. Public Health Implications

6.9.1. None.

7. Ward Members Affected

7.1. Affects all Members.

8. Consultation & Engagement

8.1. None required.

9. Access to Information

9.1. Section 46 of the FOIA

<https://ico.org.uk/media/1624142/section-46-code-of-practice-records-management-foia-and-eir.pdf>

9.2. Data Protection Act 2018

http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

9.3. Article 5 of the GDPR

<https://gdpr-info.eu/art-5-gdpr/>

10. Contact Information

10.1. Any questions relating to this report should be directed to the following officer:

Name: Gareth Pawlett

Job Title: Corporate Manager (ICT) and Chief Information Officer (CIO)

Email: Gareth.pawlett@cheshireeast.gov.uk