



North Devon District Council

## Internal Audit Report

### Email & Exchange Server 2018/19

January 2019

This report has been prepared on the basis of the limitations set out on page 21.

**Report issued to:**

Chief Executive	Mike Mansell
Head of Resources	Jon Triggs
Business Information Systems Manager	Nina Lake
Senior Technical Analyst	Paul Shears



# Contents

Executive Summary .....	1
Audit Opinion & Summary of Findings .....	2
Appendix A – Audit Framework .....	11
Appendix B – Reporting Definitions .....	12
Appendix C – Staff Interviewed.....	13
Statement of Responsibility.....	14

This report (“Report”) was prepared by Mazars LLP at the request of North Devon District Council and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

This Report was prepared solely for the use of North Devon District Council and to the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification. Accordingly, any reliance based on the report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk.

Please refer to the Statement of Responsibility in Appendix D of this Report for further information about responsibilities, limitations and confidentiality.

# Executive Summary

## Background

North Devon District Council (NDDC), like all other organisations relies on e-mail as a primary means of communication with the public, internally and with other partnership bodies to help support critical operations as well as delivering business as usual (BAU) functions.

Poor design of the e-mail and the Microsoft exchange environment, may compromise the confidentiality, integrity or availability of the system which may result in reputational risk to the Council or loss of personal, sensitive or confidential data. Absence of e-mail communications may also restrict the Council's ability to deliver services and effectively communicate.

Currently the Council operate two e-mail systems, the normal GOV.UK e-mail used for public sector organisations and the secure GCSX e-mail which they use to send secure files (only secure if the recipient is on the GCSX network, as the GCSX e-mail is not transmitted over the internet as such, but is transmitted over the PSN). It has been noted that use of the GCSX email is due to cease in March 2019 and in preparation for this the Council have formal plans to move to Office 365 prior to March 2019.

Currently the Council are utilising Exchange 2013 on premise with all incoming and outgoing e-mail scanned for virus, malware and spam by Symantec message labs software.

# Audit Opinion & Summary of Findings

Through the work undertaken, the following opinion has been provided:

## Audit Opinion



**Limited Assurance**

Weaknesses in the system of controls are such as to put the system objectives at risk, and/or the level of non-compliance puts the system objectives at risk. For a key to the assurance ratings, see Appendix B – Reporting Definitions.

## Summary of Findings

As a result of this Internal Audit, we have raised the following recommendations:

Priority	Number of Recommendations	Area of Scope / Recommendation
	0	
	3	<i>Email Policy</i> <i>Email Management</i> <i>User Access</i>
	1	<i>Email Security</i>

# Section 1 – Detailed Summary of Key Findings

## Area 1: E-Mail Acceptable Use Policy and Procedures

There is a clearly defined Email policy in place applicable to all employees, elected members and any individual or partnership organisation. The policy includes acceptable usage of email, compliance, defined roles and responsibilities, confidentiality, email monitoring arrangements and security awareness with regards to spam emails, viruses and phishing. The policy is disseminated to all staff at induction and is also available on the Council intranet, however, we noted that there is no formal ongoing awareness raising or refresher training given to users following initial receipt. Therefore, a recommendation had been raised. **(Recommendation 1)**

The Email policy was produced in 2016 and formally approved by the Senior Management Team in 2017. It has recently been reviewed (May 2018) and updated to reflect the new General Data Protection Regulation (GDPR).

We also noted that an appropriate legal disclaimer which protects and limits Council liability was in use on and appended to outbound emails from the Council. This defines the contents as confidential and deters abuse by warning and raising awareness of the email monitoring arrangements in place.

## Area 2: E-Mail Management

E-Mail message management, administration rules and policy settings were appropriately established and applied on the Exchange Server 2013 platform with a 51MB limit applied to email messages and attachment size.

The Council have set size limits to individual mailboxes which range between 1.5 and 4 Gb (Gigabytes). However, we noted that no standardised Exchange mailbox size storage policy has been formally established, agreed or formally documented within the ICT Email Policy. Furthermore, through enquiry with the Senior Technical Analyst we noted that there is no archiving or formal records retention schedule set within the email and exchange server. This is primarily due to the fact that the current licensing arrangements do not allow for the use of PST (Personal Storage) files for export of emails to local file storage. Effectively the email system is being utilised as a storage system which in itself creates a risk with regards to data protection and also due to the current disaster recovery (DR) arrangements there is the potential for significant data loss in the event of disaster. **(Recommendation 2)**

## Area 3: E-Mail Security

Access to the Outlook email client and Exchange mailbox was restricted to users with a valid Council Active Directory (AD) network login which adhered to the requirements of the IT Security Policy established at the Council. Furthermore, powerful high level administrative access to the Exchange infrastructure was restricted to the in-house IT Infrastructure Team plus one account for the Antivirus provider Clarinet. Exchange roles assigned were commensurate with the job, restricted to individual user accounts with accountability and transparency in place.

The use of encryption was not enforced using the local Exchange 2013 and Outlook email system, however, the email policy does make clear under section 8.2 that *“Files containing Restricted information as defined in the Council’s IT Acceptable Usage policy, or containing personal information about an individual, must never be transferred using email without encryption. If there is a business need for any such information to be transferred using email, the ICT Service Desk must be consulted to ensure that an approved process is followed”*. However, given that staff may only see this policy at induction they may not be fully

aware of the correct procedure to follow (see **Recommendation 1** Awareness of Council Policy). Support is also available from the ICT Service Desk when handling and transmitting sensitive and confidential information contained in emails.

We noted that the current e-mail system does not fully meet the Governments Digital Service guidelines. Which include the following best practice and can be located at the following address <https://www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing>:

- The email service is capable of sending and receiving email using Transport Layer Security (TLS) – TLS is an encryption protocol used to protect data in transit between computers. When two computers send data they agree to encrypt the information in a way they both understand.
- Domain-based Message Authentication, Reporting and Conformance (DMARC) – DMARC) is an email standard that checks that inbound emails came from where they say they came from using a combination of Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). It also tells the recipient’s email service what to do with emails that fail the check and asks recipient email services to send back reports of where the email is coming from
- Sender Policy Framework (SPF) – SPF validates the email domain a message was sent from by listing valid sending IP addresses or domains in the DNS record. This lets recipient email services check if an email came from a valid IP or domain and mark it as spam if it didn’t.
- Domain-Keys Identified Mail (DKIM). – DKIM verifies the domain an email came from and helps show that it hasn’t been tampered with in transit. The receiving email service can then filter out email that fails the DKIM check.

At present from the above key areas the Council have applied SPF and TLS. Currently DMARC and DKIM are not applied.

We also noted that the Council does not use any 3<sup>rd</sup> party secure file sharing tools such as Egress, Cryptshare or Huddle. To share sensitive files the Council is encouraging staff to password protect documents when needed (**Recommendation 4**). We noted there is very little value in implementing anything additional in line with the above, as these should be addressed when migrating to and implementing Office 365

#### **Area 4: E-Mail Usage Monitoring and Virus Controls**

The Council are using Kaspersky anti-malware endpoint protection for desktops and laptops. Emails are screened using Symantec provided by Claranet. Anti-virus and anti-spam reports are provided weekly by the supplier and reviewed, investigated and remediated by ICT at the Council.

To allow access to email from mobile phones, the Council are using Active Sync and Kaspersky and are reliant on the phone’s operating system standard security. However, it has been noted a business case has been approved and funded for the Council to move to “Airwatch MDM” as part of the migration to Office 365, which will further improve control, security and resilience.

Email traffic containing attachments are scanned for content, viruses, phishing, malicious software and spam, as per the policies defined at the Council. This is performed at the external perimeter by the third-party contractor (Symantec Cloud based managed service) on behalf of the Council. Anti-virus protection was up-to-date on the email server and updates of the latest virus signatures deployed.

In addition to an annual IT Health Check assessment carried out by a 3<sup>rd</sup> party provider (Sapphire), the Council also receive quarterly vulnerability scans of their internal networks to ensure they remain aware of their current position with regards to known vulnerabilities and patch updates and can take appropriate action

where necessary. The Council have developed an action plan to address the vulnerabilities highlighted in the reports and continue to update and action as appropriate.

### Area 5: Back up & Recovery

The Exchange Server is backed up onsite, however, there is no replicated Exchange server at the back up location (Lynton House). Therefore, if the primary data centre were to be lost in the event of a disaster then there is the potential for all new e-mails to be lost and a delay in accessing existing e-mails. The risk to data loss is increased due to the way that the Council are currently using the email system as a storage facility. It has been noted that whilst the Symantec scanning software retains emails for up to 5 days, the council would need to rebuild a server within that timescale. Given the previous issues raised with regards to Business Continuity and Disaster Recovery in previous audit reports (no full DR test has been carried out, no prioritisation of service restore agreed by the Council to enable the DR plan to be updated and no firewalls at the back up facility), there is no guarantee that this timescale is achievable or that it would be effective. Given that Email is key to effective communication both internally and externally at the Council there are a number of potential issues that need to be considered as part of the Disaster Recovery process for example, is the exchange server rebuild process documented and who would take responsibility, has additional funding been identified should it be required, and would the rebuilt server run efficiently, as without restore testing the back-ups may be corrupt.

It has been noted that with a move to Office 365 some of the risk would be mitigated because of the move to a cloud.

Given that Business Continuity and Disaster Recovery has been covered extensively in previous audits, is high priority on the risk register and the Council continue to address this issue **no recommendation** has been raised within this report.

### Area 6: Change Control

Whilst access to the Exchange administration console is restricted to authorised users only, it has been noted that there are no formal change control procedures in place. For example, if a member of staff terminates employment from the Council, a line manager may request access to their mail box to obtain information otherwise unavailable, however once IT have granted access there is no process to limit how long access is granted for or that access is removed. Failure to remove access may lead to the continued inappropriate access to personal or sensitive information. Therefore, a recommendation has been raised **(Recommendation 3)**

## Section 2 – Recommendations / Matters Arising

### 1. Email Policy

Priority 3

Recommendation	Rationale	Responsibility
<p>Continued awareness raising and refresher training on Council policy should be undertaken annually as a minimum. This could be in the form of emails to staff, updates on the intranet or formal training sessions.</p> <p>Management should consider revising the line in section 5.2 of the policy which reads “Any email which has a subject line of “Unison Private and Confidential” will not be inspected”. To provide further clarification as to the Council’s position in relation to the monitoring of emails and to ensure this caveat is not used inappropriately.</p>	<p>Continued awareness ensures all staff adhere to the Council’s current working arrangements, legal requirements and individual responsibilities.</p> <p>We noted that there are a number of policies and procedures in relation to ICT services within the Council; these include, Information Security, Email, Internet Acceptable Usage (next review in 2019). However, staff are only presented with these policies at induction or at the time of review (potentially every 3 years depending on the review schedule).</p> <p>By highlighting the fact that there are exceptions to the rule it could result in misuse of the system, and inappropriate mails could be sent under the guise of Unison business or marked as “confidential”.</p> <p>If staff are not reminded of the Council policies, they may not be fully aware of the responsibilities and could potentially be working to out of date practices, putting themselves and the organisation at unnecessary risk of reputational damage, legal implications and financial risk.</p>	<ol style="list-style-type: none"> <li>1. Business Information Systems Manager</li> <li>2. Senior ICT Project Support Officer</li> <li>3. HR Manager</li> </ol>
<b>Management response</b>		
<p><b>Agreed:</b></p> <ol style="list-style-type: none"> <li>1. With the already commenced migration of emails to Office 365, we will use this as an opportunity to refresh staff on their responsibilities in relation to e-mails and the associated policies.</li> <li>2. We will schedule dates in the ICT Service Desk to prompt some form of communication on e-mail good practice.</li> <li>3. The Email, Internet &amp; Acceptable Usage Policy will need to be revised as GCSX mail will no longer be available by the end of March 2019 and our move to Office 365. Changes to this policy will need to be approved initially by Workforce Matters (Unison) where we can highlight this risk and request that this is removed.</li> </ol>		<p>May 2019</p>



## 2. Email Management

Priority 2

Recommendation	Rationale	Responsibility
<p>Management should consider agreeing and applying formal retention periods to the mailbox settings and document this as part of the Email Policy to encourage staff to manage these more efficiently.</p> <p>The Council should also inform staff that email is not to be used as a storage function and any sensitive documents or emails that need to be retained should be stored within the Council's secure network folders.</p> <p>We noted that due to the current licensing arrangements the export of email is currently unavailable as they do not have the authority to utilise PST files as part of the agreement with Microsoft.</p>	<p>By formally documenting retention periods to the mail box, it will prompt staff to periodically cleanse their individual mail box and discourage staff from storing information inappropriately and for longer than is necessary.</p> <p>We noted that the Council have not formally documented or applied retention periods within the exchange server or the ICT Email Policy. Furthermore, through enquiry with the Senior Technical Analyst we noted that there is no archiving or formal records retention set within the email and exchange server, this is primarily due to the fact that the current licensing arrangements do not allow for the use of PST files for export of emails to local file storage. Effectively the email system is being utilised as a storage system which in itself creates a risk with regards to data protection and also due to the current DR arrangements there is the potential for significant data loss in the event of disaster.</p> <p>It should be noted that some of the above risk will be mitigated with a move to Office 365 however it will still need to be managed appropriately and in line with updated Council policy and procedure.</p>	<p>Senior Management Team</p>
<b>Management response</b>		
<p><b>Agreed:</b></p> <p><u>That SMT discuss the viability of applying a formal retention period to the mailbox settings, plus an agreed phased approach of reducing this retention period of a phased time.</u></p> <p>SMT to advise their teams that:</p> <ol style="list-style-type: none"> <li>1. Their e-mail should not be used as a storage function for sensitive documents/information,</li> <li>2. They need to apply the same formal retention periods they apply to their information asset registers.</li> </ol>		<p>Ongoing</p>

<p>As Phase II of our move to Office 365 we intend to look at the feasibility of moving away from our traditional team / corporate drives and moving to SharePoint, but again staff would need to ensure that the information they were transferring was categorised and time bound.</p>	
--	--

### 3. Access requests and changes to the mailboxes

Priority 2

Recommendation	Rationale	Responsibility
<p>A formal process should be developed to ensure that any changes to the email and exchange service are formally documented and authorized appropriately. This includes requests for access to mailboxes (to include access requests following termination of employment) and also removal of temporary access. Access should only be granted if there is a justified business need and should only be granted for a set period of time (up to 30 days following termination for example).</p>	<p>Having a documented change and access process will enable the ICT department to more efficiently manage user access to accounts following staff termination or removal of temporary access.</p> <p>From enquiry with the Senior Technical Analyst, we noted that if access is granted to a user following termination or as a temporary access request there is no formal procedure to review or remove access after a set period. As a result, the process currently relies on line managers to inform them once access is no longer required. It was also noted that managers are requesting access permanently</p> <p>Without a sufficient review process in place, there is a potential risk of inappropriate access to Council information systems and/or personal/sensitive data which could result in reputational damage, legal action and potential financial loss.</p>	<p>Senior ICT Project Support Officer</p>
<p><b>Agreed:</b></p> <p>All requests will be asked to advise why they require access and for how long, these will then be discussed at our Change Advisory Board (CAB), decisions documented on our Service Desk and termination dates set and followed through to ensure access or closure of those accounts are actioned.</p>		<p>Complete</p>

#### 4. E-Mail Security

Priority 2

Recommendation	Rationale	Responsibility
<p>Security settings should be reviewed as part of the Office 365 implementation project to ensure they align with the NSCS email security guidance and all the relevant controls are applied.</p> <p>Consideration should also be given to utilising an encrypted file sharing application if and when confidential or sensitive files need to be shared outside the Council or Government networks.</p>	<p>We noted that the current e-mail system does not fully meet the Governments Digital Service guidelines. Which include the following best practice and can be located at the following address <a href="https://www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing">https://www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing</a>:</p> <ul style="list-style-type: none"> <li>• The email service is capable of sending and receiving email using Transport Layer Security (TLS);</li> <li>• Domain-based Message Authentication, Reporting and Conformance (DMARC);</li> <li>• Sender Policy Framework (SPF);</li> <li>• Domain-Keys Identified Mail (DKIM).</li> </ul> <p>SPF and TLS is applied however only after the e-mail leaves Symantec's Message Labs software. They do not currently apply DMARC/DKIM. There is very little value in implementing anything additional in line with the above, however all of the above should be considered, when migrating and setting up Office 365.</p> <p>We also noted that the Council does not use any 3rd party secure file sharing software like Egress, Cryptshare or Huddle. To share sensitive files the Council is encouraging staff to password protect documents when needed.</p>	<p>Senior Technical Analyst</p>
<b>Management response</b>		
<b>Agreed:</b>		April 2019

We are moving to Office 365 to ensure we align with the NSCS e-mail guidance and plan to start off giving very limited access to ensure that we apply the correct rules and appropriate controls. To mitigate the loss of GCSX mail, we also plan to use the Office 365 Message Encryption (OME) when the business wants to send sensitive business information.	
--	--

## Appendix A – Audit Framework

### Audit Objectives

The audit was designed to ensure that management have implemented adequate and effective controls over Cyber Security at North Devon District Council.

### Audit Approach & Methodology

The audit approach was developed with reference to the Internal Audit Plan and by an assessment of risks and management controls operating within each area of the scope. The following procedures were adopted:-

- Identification of the role and objectives of each area;
- Identification of risks within the systems, and controls in existence to allow the control objectives to be achieved; and
- Testing of controls within the systems.

From these procedures we have identified weaknesses in the systems of control, produced specific proposals to improve the control environment and have drawn an overall conclusion on the design and operation of the system. See Appendix B for details of the Audit team and staff interviewed.

### Areas Covered





Audit work was undertaken to cover the following areas and control objectives: -

- Email Policy & Procedures
- Email Security
- Email Mailbox Management
- Email Monitoring & Virus Scanning
- Back up & Recovery
- Change Management

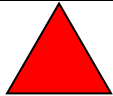

## Appendix B – Reporting Definitions

In order to assist management in using our reports:

a) We categorise our **audit opinion** according to our assessment of the controls in place and the level of compliance with these controls:

	<b>Full Assurance</b>	There is a sound system of control designed to achieve the system objectives and the controls are being consistently applied.
	<b>Substantial Assurance</b>	While there is a basically sound system, there are weaknesses which put some of the system objectives at risk, and / or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.
	<b>Limited Assurance</b>	Weaknesses in the system of controls are such as to put the system objectives at risk, and/or the level of non-compliance puts the system objectives at risk.
	<b>Nil Assurance</b>	Control is generally weak, leaving the system open to significant error or abuse, and/or significant non-compliance with basic controls leaves the system open to error or abuse.

b) We categorise our **recommendations** according to their level of priority.

	<b>High Priority Recommendation</b> Major issues that we consider need to be brought to the attention of senior management and the audit committee.
	<b>Medium Priority Recommendation</b> Important issues which should be addressed by management in their areas of responsibility.

**Low Priority Recommendation**

Detailed problems of a minor nature resolved on site through discussions with local management.

## Appendix C – Staff Interviewed

Audit Team	Staff Consulted
Mark Towler – Engagement Director	Nina Lake – Business Information Systems Manager
Rachel De Bradeny – Engagement Manager	Paul Shears - Senior Technical Analyst
John Wakefield – IT Audit Manager	
Contact Details: Rachel.DeBradney@mazars.co.uk	

An exit meeting was held with the Business Information Systems Manager and Senior Technical Analyst in November 2018.

### Acknowledgement

We would like to thank the Management and staff involved in the audit work for their assistance.

## Statement of Responsibility

We take responsibility to North Devon District Council for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

Registered office: Tower Bridge House, St Katharine's Way, London E1W 1DD, United Kingdom. Registered in England and Wales No 0C308299.