Information Security Document

Secure Email Policy

Version 7.0

Version History			
Version	**Date**	**Detail**	**Author**
1.0	27/09/2013	Approved by Information Governance Group	Jo White
2.0	03/11/2014	Reviewed by Information Governance Group	Jo White
3.0	15/12/2015	Reviewed by Information Governance Group. Remove Elected Members from breaches section.	Jo White
4.0	11/09/2017	Reviewed by Information Governance Group. Amended to take in to account the changes to the availability and licensing of Microsoft 365 encrypted email.	Jo White
5.0	10/09/2018	Reviewed by Information Governance Group. Changes to GCSx email operation.	Jo White
6.0	08/04/2019	Reviewed by Information Governance Group. Deletion of GCSx and new ability to send secure emails via TLS.	Jo White
7.0	14/04/2020	Reviewed by Information Governance Group. Alterations to the use of CJSM emails and secure emails button.	Jo White

This document has been prepared using the following ISO27001:2013 standard controls as reference:	
ISO Control	**Description**
A.9.4.4	Use of privileged utility programs
A.12.1.1	Documented Operating Procedures
A.13.2.1	Information Transfer Policies and Procedures
A.13.2.3	Electronic Messaging
A.14.1.2	Securing application services on public networks
A.18.1.3	Protection of records.
A.18.1.4	Privacy and Protection of personally identifiable information
A.18.2.3	Handling of assets

1 Introduction

The security of electronic information is critical in today's environment, with potential interception of unsecured email sent over the internet being a realistic possibility. To mitigate this risk, any electronic information considered restricted or sensitive should be secured by encryption when being sent to recipients. As such, all Derbyshire County Council employees, including elected members, partner agencies, contractors and vendors with access to Council systems are responsible for taking the appropriate steps, as outlined below, to use the correct method of sending emails securely.

2 Purpose

The purpose of this policy is to define the Council's agreed methods for sending emails securely. Other established government secure email systems are in use but a large proportion of the private population do not have access to these. The Council has therefore adopted encryption solutions for sending email securely to external parties. Using an encrypted solution ensures that the content of a message is securely delivered to the intended recipient. Even if messages are intercepted the content/s cannot be read due to encryption being applied - essentially scrambling the content/s of the email whilst in transit.

3 Scope

This policy applies to all employees, elected members, contractors, vendors and partner agencies who:

- have or are responsible for sending personal and sensitive data to parties external to the Council in the course of conducting Council business.
- have or are expected to receive personal and sensitive information from external parties in the course of Council business.

4 Policy Statement

It is currently not possible to use one secure email solution to fit all circumstances. The following options are available to the Council for sending secure encrypted emails:

4.1 CJSM Secure Email

CJSM is widely accepted by the Law Courts and email can be sent to and from an existing @derbyshire.gov.uk mailbox, but can only be sent securely to an existing CJSM email address. There is also an administrative overhead which requires the email addresses to be created via a third party internet based portal.

- A small group of administrators exist for the CJSM at the Council who can set up new accounts and reset passwords : -
    - Administrator for Legal Service and Call Derbyshire – Jo White
    - Administrator for Youth Offending – Dawn Dickens

- A temporary password is initially created for an individual User by the CJSM system. A User will be informed of the temporary password which must be changed immediately and constructed in accordance with the Council's Password policy. CJSM passwords expire after 90 days

- Emails cannot be sent or received if the account is not kept active by the authorised individual. If accounts lapse, they can only be re-activated through application to one of the administrators.

- The username will be the individual's @derbyshire.gov.uk email address accompanied by the password.

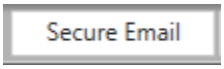
- The Council's Information Security Team will be responsible for handling requests for secure CJSM email accounts.

4.2 Forced Secure TLS

This does not require any special software or email setup, only a @derbyshire.gov.uk email address. Forced TLS will attempt to send email securely but can only work if the recipients email system is able to accept email sent using TLS. If an email recipient does not support TLS, a 'Non-Delivery' notification will be sent to the ~~user~~ sender but only after 24 hours.

- 'Forced Secure TLS' should be used to send emails securely to external agencies/individuals if the email has been classified as restricted.

- It can be activated by clicking on the 'Secure Email' (forced TLS) option available as a button when creating a new email:



- New organisation or individual recipients can be sent a test email via 'Forced Secure TLS' (as above) to ensure the recipient is able to accept TLS emails.

- Urgent emails, where the user does not know the recipient's email system is capable of accepting emails sent using TLS and cannot wait 24 hours for a non-delivery notification, should choose the Microsoft 0365 Email Encryption Service (4.3 below).

4.3 Microsoft 365 Email Encryption Service (OME).

This does not require any special software or email setup by the sender, only a @derbyshire.gov.uk email address.

- Microsoft Office 365 Email Encryption is available by clicking on the button when creating a new email. This should be used to send emails classified as restricted securely to external agencies/individuals that do not use CJSM email or to those who cannot receive emails via the 'Secure Email' button as described in 4.2 above

- External recipients of Microsoft 365 Email Encryption will be able to open the message either by logging into a Microsoft Account or by receiving a 'one-time passcode' which is automatically sent from the sender. The recipient will be able to view and reply to Council encrypted message emails on a secure Microsoft web page. The chain of replies between the Council and the recipient will remain encrypted

5 Responsibilities

- Emails containing personal or sensitive information must be sent securely using the encryption methods described in this policy.

- All senders must ensure the appropriate secure email method is chosen according to the circumstances of the destination of the email. See Appendix I.

- Senders of any controlled/restricted email must be extremely vigilant about the recipients email address, so as to not send any sensitive data to the wrong individual/s. Senders of controlled/restricted emails, via any of these methods, must ensure they have and use the correct recipient email address.

- The use of web-based email systems (available via the internet) (such as Hotmail,) and cloud-based storage systems (such as Dropbox) or any system of email/storage not authorised by the Council is not permitted.

6 Compliance with legal and contractual obligations

Data protection is of concern regarding secure email as any sensitive data sent via email that is not sent on a secure system is open to interception as the email travels across the internet to the recipients email systems. By sending this information by a secure email service only the intended recipient will be able to access the data and hence mitigate the risk of being fined by the Information Commissioners Office for breaches of the Data Protection Act.

7 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council assets, or an event which is in breach of the Council's security procedures and policies.
All employees, elected members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council.

In the case of third party vendors, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Council's ICT systems or network results from the non-compliance, the Council will consider legal action against the third party. The Council will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an individual the matter may be dealt with under the disciplinary process.

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.

APPENDIX I

Secure e-mail solution	Cost	Maintenance/setup	Accessibility with DCC systems	Accessibility outside the authority	Risk of exposure
CJSM	Low	Medium – departmental administrator maintains a list of users	Good – is used from same email account (a ~~D~~@derbyshire.gov.uk mailbox).	Medium – only CJSM accredited bodies can access this email system. Requires a specific infrastructure setup.	Medium – email sent from a user not setup for CJSM or to a non CJSM address will not be transmitted securely.
TLS	Low	Low – it is a standard on all Council email accounts.	Good – the secure email is sent from the same Council email account (A @derbyshire.gov.uk email account)	High – anyone who uses email capable of secure TLS email.	Low – An attempt will always be made to send the email securely. With a notification being sent back to the sender if the email could not be sent.
365 Email Encryption	Low	Low – it is standard on all Council email accounts.	Good – the secure e-mail is sent from the same @derbyshire.gov.uk email account (by using an e-mail template).	High – anyone can use this system with an internet connection.	Low – if an email template is used the message will always be sent securely.