Torfaen County Borough Council

Email Policy

Version 1.0 Live

DOCUMENT CONTROL

Title:	**Email Policy**		
Document Owner:	**Senior Information Risk Owner** (SIRO)		
Document Author:	**Sharon Clifford**		
Reference:	**IG025**	**Retention Period:**	**Until next review**
Document Classification:	Official	**Location:**	SWOOP
Version / Status:	Live	**Approved by:**	IAOG/Leadership Team
Current Issue Date:	June 2023	**Next Review Date:**	June 2024

REVISION HISTORY

Issue Date	Version / Status	Reason for Change	Changed By:
June 2023	1.0 Live	Policy Implementation	Sharon Clifford

TABLE OF CONTENTS

1. PURPOSE

Email messages are an important means of communication which enable the Council to provide better customer service. However, email is subject to Data Protection Law and Freedom of Information legislation as it contributes to corporate records in the same way as traditional methods of communication such as telephone calls, letters or forms. It must also be remembered that Email communication is another form of publishing and libel laws apply. This Policy and accompanying Procedure will provide clarity on the use of email for business and the corporate standards to follow.

The purpose of this Policy is to:

- Provide clarity on the use of email for business purposes
- Remind staff that email is a component of Records Management
- Explain the corporate standard email format to use
- Refer users to the relevant guidance available including IG025(A) Email Procedure document

2. SCOPE

This policy applies to all emails created, received and processed by the Council and:

- All employees, whether office based or working via remote access, including contractors, volunteers, agencies and partner organisations operating on behalf of the Council.
- All elected members whilst working on Council business.

3. AIMS & OBJECTIVES

To ensure a robust Email process is in place which meets Retention guidelines and complies with, amongst others, IG006 Acceptable Use Policy and IG006(A) Procedures, IG007 Data Protection Policy and IG007(A) Procedures and IG013 Records Management Policy. The following applies equally to individual corporate email accounts as well as group/team inboxes managed by staff as well as those where proxy access to an inbox has been provided.

Corporate Standards

You must comply with the standards laid down by the Council for communication methods and ensure your content is appropriate, you should refer to the Corporate Standards - Procedures and Guidelines for the Use of Email on SWOOP https://swoop.torfaen.gov.uk/en/Document-Library/OS-Guidance/ProceduresGuidelines-UseofE-Mail.pdf Please note this has not been updated since 2011 and is currently being reviewed.

Use of Email

Email is critical to the business of the Council and can be monitored as the information contained belongs entirely to the Council as it goes through our network. People who have been granted access to our systems will be given a Council email address purely for business purposes use.

You must familiarise yourself with the accompanying IG025(A) Email Procedures document, IG006 Acceptable Use Policy and specifically IG006(A) Acceptable Use Procedure document which details unacceptable actions.

Security of Email

Significant expenditure and resources are dedicated to protecting the Corporate network from external threats and ensuring business continuity so that the Council can provide services to its residents. All staff have a responsibility to ensure they comply with the relevant Policies and Procedures and be aware of the implications of their own actions when using email.

Staff should be especially vigilant for phishing emails which seem plausible but request information, and emails containing links or attachments that could introduce malware/viruses to the network. Please read the Information Security Policy IG019 and the Cyber Awareness page on SWOOP Cyber & Information Security - Swoop, the Intranet for Torfaen Employees

Where personal information needs to be sent by email you must follow the steps in the accompanying Email Procedure document.

Retention and Records management

Emails are corporate records and subject to retention periods which will be determined by their content and topic:

- Where they are deemed necessary to retain as part of a record, they must be saved to the relevant system (eg M Drive/WCCIS/IDOX) as soon as possible. Please see the Guidance document explaining the method to save these messages Changes to Email Retention is Coming! (office.com)
- The Outlook email system is not to be used as a filing system and will soon have an auto-deletion facility enabled which will delete all emails past the set retention period. Please ensure you read the communications sent to all staff advising the implementation date and the retention period involved.

4. RESPONSIBILITIES

The following individuals/groups have specific responsibilities:

Senior Information Risk Owner (SIRO)	Overall executive responsibility for the Email policy and standards and their application throughout the Council

Data Protection Officer	To monitor and promote compliance of the Email policy and report back to the service areas via Leadership Team Review, implementation, and governance through the Information Asset Owner's Group (IAOG)
Data Protection and Information Governance Team	Policy formulation and review and providing advice and guidance Ensuring that the Email policy (and any related procedures and standards) are kept up to date and relevant to the needs and obligations of the Council
Chief Information Security Officer CISO	Ensuring the security and safety of our systems and infrastructure and reporting any breaches to the SIRO. Can be contacted via security@torfaen.gov.uk
Heads of Service/Line Managers	Ensuring that these Policies & Procedural documents are made known to all staff, inclusive of agency workers, contractors, volunteers, students or anyone accessing the Council's systems or information and in doing so ensuring awareness of their responsibilities for the use of Email To assign clear responsibility for information which passes out of their control following (for example) restructuring, moving of functions, closing of projects
All staff and elected members	Reading and adhering to the Email Policy and related procedures/guidance when managing, storing and disposing of the information they create and receive during the course of their duties To undertake any training/awareness provided To ensure that the information held by the Council is disposed of appropriately and that all sensitive information is disposed of securely To report immediately any observed or suspected incidents where sensitive information has or may have been insecurely disposed of Documenting of processes and evaluating procedures within their service areas
Systems Administrators	Management of the data systems in their service area in conjunction with SRS technical staff. System-specific procedures should be made available to all staff using specialised service area systems such as (but not limited to) WCCIS/Civica/etc.

Shared Resource Service (SRS)	Managing the network infrastructure, ensuring system continuity and security
Gwent Archives	Gwent Archives is the Accredited Archive Service for Torfaen County Borough Council. It will work with teams to select and store records for permanent preservation according to the Torfaen County Borough Council retention schedule as well as the Gwent Archives Collections and Appraisal Policies. Contact details for the team are on their website at www.gwentarchives.gov.uk

5. LEGISLATION & KEY REFERENCE DOCUMENTS

(Please note this list is not exhaustive)

The Council will abide by all relevant UK legislation and the following policies and procedures:

- UK GDPR (General Data Protection Regulation)
- The Data Protection Act (2018)
- The Copyright, Designs and patents Act (1988)
- The Computer Misuse Act (1990)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Social Services & Well-being (Wales) Act 2014
- Children Act 2004 / 2019
- Equality Act 2010
- Crime and Disorder Act 1998
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (amended 2019) PECR
- Welsh Language Standards

TCBC POLICIES

- IG007 Data Protection Policy
- IG001 Information Governance Framework
- IG002 Information Governance Strategy
- IG003 Information Governance Policy
- IG006 Acceptable Use Policy
- IG019 Information Security Policy
- IG017 Information Sharing Policy
- IG013 Records Management Policy

- IG020 Retention Policy
- IG022 Information Secure Destruction Policy
- IG010 Information Access Policy
- IG012 Information/Data Loss Policy
- IG021 Requests for Information Policy
- IG011 Clear Desk Policy
- IG016 FOI Policy
- IG008 Password Policy
- IG025 Version Control Policy
- IG023 BYOD Policy
- IG009 Social Media Policy
- Dignity at Work Policy

TCBC PROCEDURES

- IG007 (A) Data Protection Procedures
- IG101 (A) Offsite Archive & Destruction Procedures
- IG021 (A)(B) Requests for Information Procedures
- IG008 (A)Password Construction Procedures
- IG020 (A)(B) Retention Schedule (on SWOOP)
- IG023 (A) BYOD Guidance
- IG006 (A) Acceptable Use Procedures
- IG025 (A) Email Procedures
- Social Media Guidance
- Code of Conduct for Employees
- Procedures and Guidelines for the use of Email

6. MONITORING AND REVIEW

The Information Management Groups are responsible for reviewing the content and ensuring that policies are published on the Information Management site on SWOOP. This Policy will be subject to review when any of the following conditions are met:

- Content errors or omissions are highlighted.
- Where another standard/guidance issued conflicts with the information in this policy.
- An initial 1 year review from policy implementation and on a 3 yearly basis from the current version approval date.

7. COMPLIANCE

Failure to comply with this policy may be regarded as misconduct and investigated under the Council's Disciplinary Rules and Procedures. In serious cases this may be

considered gross misconduct and lead to dismissal from the Council's employment without notice or payment in lieu of notice. In serious cases individuals may be liable for prosecution under Data Protection Law