



Information Security Management

Egress Workspace – Conditions of Use for Council Staff and Members

1. Introduction

This document defines the Council's conditions of use for the Egress Secure Workspace (Egress) system.

The Council has commissioned a secure, Government-accredited 'file-sharing and collaboration portal' (website) from Egress – Egress Switch Secure Workspace. This allows Council Users to share sensitive files and work securely with other Agencies, Partners, Vendors and Third Parties.

Each Council team utilising Egress is allocated their own 'Workspace.' A Workspace is a secure area within Egress, which can only be seen by users who have been granted access.

Access to Egress is available from any internet-connected device.

2. Scope

All employees, agency workers, contractors, members, and temporary staff such as work placements ('users') who wish to utilise Egress are obliged to adhere to the Conditions of Use within this document.

3. Conditions of Use

3.1 Acceptable Use Policy

This document supplements, and should be read in conjunction with, the Council's Acceptable Use Policy.

For the avoidance of doubt, Egress is considered a Council Information System.

Reference:	IS20130422-001	Version:	1.6
Protective Marking:	Official	Status:	Final
Author:	IT Governance & Security	Page(s):	1 of 3
Last Reviewed on:	25 January 2024	Next Review Date:	25 January 2025



3.2 Sensitive Information

Egress can be utilised to store sensitive information up to the classification OFFICIAL-SENSITIVE.

3.3 Use of Egress for personal and other purposes

Each Egress workspace has been provisioned by the Council for a specific purpose (for example, sharing sensitive information with a third party).

The Workspace must not be utilised for any other purpose, including personal file-sharing or collaboration.

3.4 Workspace Owners

Each Egress Workspace must be owned by one or more Council users. The owners take responsibility for:

- **What** they are sharing,
- **Who** they are sharing it with.
- **Why** they are sharing it, including ensuring that any **Data Sharing Agreement(s)** necessary are in place.
- The security of that workspace, which in practical terms means:
 - Only users who are entitled to view the information are allowed access to the workspace.
 - Providing users with the appropriate level of access they require (e.g., read-only).
 - Removing or revoking access from those who longer require it.
 - They ensure that all users comply with the relevant Conditions of Use document and the Council's Acceptable Use Policy.
 - They report any actual or suspected non-compliance of the Conditions of Use or Acceptable Use Policy to the Councils IT Service via HaloITSM.

3.5 Information Loss, Unauthorised Disclosure & Security Incidents

If information held on, or downloaded from Egress is lost or inadvertently disclosed it is the user's responsibility to report the situation as soon as practicable using the Council's Incident / Breach Management (Loss / Breach

Reference:	IS20130422-001	Version:	1.6
Protective Marking:	Official	Status:	Final
Author:	IT Governance & Security	Page(s):	2 of 3
Last Reviewed on:	25 January 2024	Next Review Date:	25 January 2025



WARRINGTON

Borough Council

of Information) processes, which can be found on the [Intranet](#).

If any other security incident occurs (for example, you believe your login details have been disclosed or utilised by someone else), the user must report this to the IT Service via HaloITSM.

3.6 Applicable Legislation

Egress is subject to the Council's obligations under the Data Protection Act (DPA) 2018, which may require the Council to disclose personal data to other bodies under certain circumstances as detailed within the Data Protection Act.

All information in Egress will be deemed to be held by the Council and hence subject to the requirements for disclosure to the public under the Freedom of Information Act and Environmental Information Regulations.

3.7 Egress Terms of Use

The Conditions of Use contained within this document are in addition to the standard Egress Secure Workspace Terms of Use.

4. Related Documents

- Acceptable Use Policy (IT Facilities & Information Security)

Reference:	IS20130422-001	Version:	1.6
Protective Marking:	Official	Status:	Final
Author:	IT Governance & Security	Page(s):	3 of 3
Last Reviewed on:	25 January 2024	Next Review Date:	25 January 2025