Document Control

Policy Title	ICT System Request
Policy Number	006-125
Owner	Information & Communication Technology Manager
Contributors	Assistant to ICT/Independent Living Senior Manager
Version	1.0
Date of Production	01 March 2016
Review date	01 March 2018
Post holder responsible for review	Information & Communication Technology Manager
Primary Circulation List	All in SHS
Web address	www.sunbeam.ie
Restrictions	None

Version Control

Version Number	Owner	Description	Circulation
1.0	Information & communication Technology Manager	New	Information & communication Technology Manager

1.0 POLICY:

This policy is in place to ensure only the necessary staff have access to various systems outlined in this policy. For the purpose of data protection, compliance and system security staff should have miminum system access as required to peform their duties. The granting of permissions and removal of permissions must be requested and approved as per this policy.

2.0 SCOPE:

This policy is for the purpose of permissions to systems as opposed to the further development of a system e.g. If a new document library is required on SharePoint it can be requested via email or having a discussion with the revelant ICT staff member, however who has permissions to this document library must follow this policy and the procedure outlined within.

The following systems are governed by this policy:

- CID
- SunbeamLink.SharePoint
- User Accounts
- Email Distribution Lists (Created/Managed by ICT)
- Server Folders/Drives

3.0 DEFINITIONS AND ACRYNOMS

Acrynoms

- **CSM**: Client Service Manager
- **SSM**: Senior Service Manager
- **SMT**: Senior Managerment Team
- **CID:** Central Information Database

Definitions

- **Sunbeamlink:** Sunbeam SharePoint Domain i.e. the name of Sunbeam SharePoint Site
- **Active Directory**: ICT system where User Account and User Groups are created and maintained.
- **SharePoint**: Microsoft SharePoint is a browser-based collaboration and document management platform from Microsoft
- **Document Library**: Sharepoint Application for saving files and folders

4.0 ROLES & RESPONSIBILITIES:

System Request Creator: Is responsible for completing a system request as per this policy. Anyone in the organisation with a sunbeam user account can/is allowed to complete a system request. Note this is the person logged into SharePoint at the time of creating a new system request.

System Request Approver: Is responsible for approving system request as per this policy. A finite list of sunbeam staff have permissions to approve a system request as outlined in the procedure sections below. System Request Approver comprise of System/Resource Owners.

ICT: Is responsible for processing approved system requests. Ensuring system requests are completed as per this policy. Only trained ICT staff in this area have permissions to carry out this work.

Owner: Sunbeam Staff member who owns a system e.g. CSM is the owner of a location distribution list, a location document library in SharePoint or a Location in CID. Department Manager is respoinsible for a department distribution list or a department document library.

User Name: This the persons(s) to whom the request applies i.e. the staff member who is being granted permission or from whom permissions is being removed. This does not need to be the same person as the person creating the request. User name will be a person(s) who already has a user account.

New User: New employee who does not yet have a user account.

5.0 PROCEDURE

For each of the above system outlined in the scope section above an 'ICT system Request Form' must be completed. Two weeks lead time is required for ICT to complete a system request. The deactivation of a user account must be request prior to the user leaving the organisation and the system request must be completed no later than the next working day the user has left the organisation and where possible should be done the same day the user leaves the organisation.

For each system outlined in the scope section above the following roles within the organisation can be approvers of a system request.

The responsibility for who has and does not have permissions to a system at any point in time is the responsible person outlined below for each system.

1. **CID** (Locations & Roles: remove and/or grant permissions)
- Accept Approval From: Location CSM, Location SSM, member of HR
- Responsible Person: Location CSM

2. **SharePoint** (Document Library, Shared Calendar, Other section of SharePoint)
- Accept Approval From: Owner or if Owner is not in the approval list owners direct line manager.
- Responsible Person: Owner

3. **Email Distribution Mailing Lists**
- Accept Approval From: Owner or if Owner is not in the approval list owners direct line manager
- Responsible Person: Owner

4. **Creation of User Account**
- Accept Approval From: Location CSM, Location SSM, member of HR, SMT or delegate
- Responsible Person: Supervisor/Manager of New Start

5. **Permanent Deactivation of User Account**
- Accept Approval From: HR
- Responsible Person: HR

6. **Temporary Deactivation of User Account**
- Accept Approval From: HR Manager
- Responsible Person: HR Manager: Note temporary deactivation is at the discretion of HR and the user's manager.

7. **Request to monitor an individual user's activity as per policy 006.095 – Information Technology Acceptable Usage Policy.**
- Accept Approval From: Managing Director (who will have agreed this with the individual's Senior Services Manager)
- Responsible Person: Managing Director
  Note: In this instance the 'User Name' in the 'ICT system Request Form' will be the Senior Services Manager of the user who is being monitored. This is who will receive the updated password of the user account in question. The approver will be the Managing Director.

Note: Active Directory Security Groups created for Locations on CID are staff location specific. SharePoint Document Library for that location will pull permission from Active Directory. Other Document Library(s) have unique permission not linked to an Active Directory Security Groups.