Government of JERSEY

Children, Young People, Education and Skills (CYPES) Policy

Title:	IT arrangements for Leavers and their Line Managers (Curriciulum Users Only)
Issued:	May 2020
Last Updated:	July 2020
Author:	Head of Governance

1. Overview

This document outlines the information governance and IT access considerations in respect of departing employees (including researchers) or departing workers (including consultants, supply staff, volunteers or agency workers) who have a Curriculum IT account – collectively referred to in this document as “Leaver”. Whilst each Primary, Secondary College and EOTAS provision operates as an individual entity, they will be referred to as “Establishment” for the purposes of this policy. The purpose of this document is to set out what should happen before and after the Leaver leaves any Establishment within the organisation where a Curriculum IT account may be utilised. This document includes the procedure that should be followed where it is known in advance of leaving that the Leaver will require IT account access after their employment/appointment ends. See flowchart at Appendix 1.

2. Recommended handover arrangments

Employees and workers must ensure that all relevant information and records are stored and managed appropriately and in line with published retention schedules. This is critical to good information management as per the Corporate “IS Policies” (see Related Documentation). All Leavers (or workers moving to another role) should discuss with their Line Manager the arrangements they have made for information handover. Line Managers and Leavers should ensure that any information and/or documents held in the Leaver’s email systems are transferred to other record keeping systems prior to leaving. This helps to retain organisational knowledge and history of decision making. Information handover arrangements could include some, or all, of the following:

- Ensuring storage of information in the relevant (and specified) areas of an Establishment’s managed storage facilities. This includes shared network drives, functional email systems or SharePoint.

- Setting up an out-of-office message on the Leaver's email account giving an alternative point of contact e.g. stating, "X has now left the establishment, please send your enquiries to person Y (email address) or person Z (email address) so that your request can be dealt with".
- Removing Leavers from limited access functional email accounts/shared folders/SharePoint.
- Changing passwords on folders containing confidential and sensitive information.

Curriculum email accounts should not be set to redirect to any personal email account. Any such re-directs will be deleted to prevent unauthorised access to information.

Mailbox contents should not be copied and kept as personal property: Email is provided for Curriculum work purposes and all communications are the property of the Establishment as specified in the Acceptable Use Policy and ICT Equipment/Facilities Conditions of Use Policy (see Related Documentation section). This principle applies to all employees/workers.

However, private and personal information that might be held in a Leaver's H:\ drive and/or OneDrive may be taken by the Leaver when they leave. This should be in agreement with an employee's line manager. In advance of their last day, Line Managers should ensure that the Leaver has complied with the above guidance.

For guidance about access or rights to created material when leaving the Establishment, the Line Manager and / or Leaver should contact the Governance team in addition to completing the Managers Leaver's Form - https://soj/Management/People/Leavers/Pages/Welcome.aspx.

3. Default situation on retention of data held in a Leaver's IT account and on their equipment

A Leaver's IT account (which includes H:\ drive, OneDrive, Outlook and TEAMs) is disabled either on the date the HR entry records the Leaver as ceasing to be employed or, in the case of an associate IT account, on the date given to IT Services by the Leaver's line manager confirming when they will cease to be employed by the Establishment. The 0365 account and mailbox contents are deleted 3 months later as per CYPES retention schedules. (Related Documentation section). Curriculum IT Support Services manage the erasure of all Establishment owned LAN devices. Where a Leaver has access to a portable (WiFi enabled) Establishment device, this must be returned to the Establishment's IT technician or Primary Learning Technologist to ensure all data has been erased.

As this is usually carried out shortly after the equipment is returned to the relevant party, information that may have been saved to the Leaver's H:\ drive or 0365 account cannot be accessed or retrieved after they have left the Establishment.

HR will provide details of Leavers to the Curriculum IT Support Services Team.

4. Extending Accces to an account

There are separate processes for:
a) requesting that a Leaver retains access to their IT account after leaving; and
b) requesting access to a Leaver's IT account after they have left.

These are set out below and are also illustrated in a flowchart at Appendix 1.

4.1 Requesting an extension to a Leaver's account before they leave

In advance of leaving, Leavers should make Establishment work and information including lessons plans and schemes of work available to colleagues and/or their line manager as part of a formal handover.

See section 2 Recommended handover arrangements above.

Be aware that it is not acceptable or appropriate for Leavers to take information that belongs to the Establishment with them when they leave. There may be instances when continuing use of the Establishment email or other systems by a Leaver after leaving is justified e.g. there is a transition period where a Head Teacher works across multiple sites (Establishments). Extending access to a Leaver's IT account beyond the end of their employment/appointment has implications for confidentiality and intellectual property. There may also be legal and contractual considerations. If it is deemed appropriate for an account extension to be put in place, the advance request shall be made as follows:

A. Any Leaver or their line manager who is requesting extension of access to IT resources should make the request formally in writing in the form of a ticket to the Curriculum IT Support Service Team;
B. This request should set out the business reasons and should specify exactly what access will be required and for and how long;
C. The Curriculum IT Support Service Manager will approve/decline or refer the request to the Director for Education (in CYPES) for approval should a concern or query arise.
D. If the Curriculum IT Support Service Manager/Director for Education (CYPES) decides to refuse the request, he/she should inform the Leaver in writing;
E. If, however, the request is approved, the Curriculum IT Support Service Manager or Director for Education (CYPES) should update the ticket within the IT Service Desk confirming and authorising the account extension request and the time period;
F. The maximum period for account extensions is three months. Only in the most extenuating of circumstances will this period be extended any request beyond three months MUST be approved by the Director for Education (CYPES);
G. If approved, the Curriculum IT Support Service Team will notify the Leaver of the end date of the extended access.

4.2 Requesting an extension to a Leaver's account after they leave

A. Occasionally a Leaver may request access to their H:\ drive or 0365 account once they have left the Establishment.
B. If advance approval has not been sought or has been sought and not granted (see 4.1 above) the Leaver should direct such requests to the Subject Access Request Point of Contact for CYPES or the subject access request page available at gov.je and follow the standard subject access procedure. (Related Documentation section).
C. A line manager or colleague may request operational access to a Leaver's emails, H:\ drive or 0365 Account after s/he has left the Establisment's employment. Any such requests must follow the "Secure Account Override" procedure (Related Documentation section).

5. Backing-up Leavers Information

Any information that has been backed up to the Azure Cloud back-up service will be kept in accordance to CYPES retention schedules (Related Documentation).

Please note that any personal information that has been backed-up within TEAMs, H:\drive, OneDrive, will be deleted three months after the deletion of any account. This information will not be able to be accessed after this time.

6. Deleted Information

Deleted information must be recorded in the Records Destruction Form and maintained by the Curriculum IT Support Services Manager. (Related Documentation Section).

7. Related Documentation

The following documents can be found on MyStates or by using the links below:

IS Policy:
https://soj/DocsForms/Policies/ModernisationAndDigital/Pages/welcome.aspx

CYPES Retention Schedule:
https://soj/Management/Records/RetentionSchedules/Pages/DeptRetentionSchedules.aspx

Acceptable Use Policy:
https://soj/DocsForms/Documents/IS/Policies/P%20IS-POL-001%20-%20Acceptable%20use%20of%20information%20systems%20and%20technology%2020161122.pdf

Subject Access Request procedure:
https://soj/SiteCollectionDocuments/Subject%20Access%20Requests.pdf#search=subject%20access%20request%20procedure

Record Destruction Form:
https://soj/DocsForms/Documents/Records%20management/RM-FORM-001%20Destruction%20Form.pdf

Cloud Computing Guidelines:
https://soj/depts/ModernisationAndDigital/Documents/ID%20IS%20guidelines%20for%20Cloud%20Computing%20v10%2020130328%20JB.pdf#search=secure%20account%20override

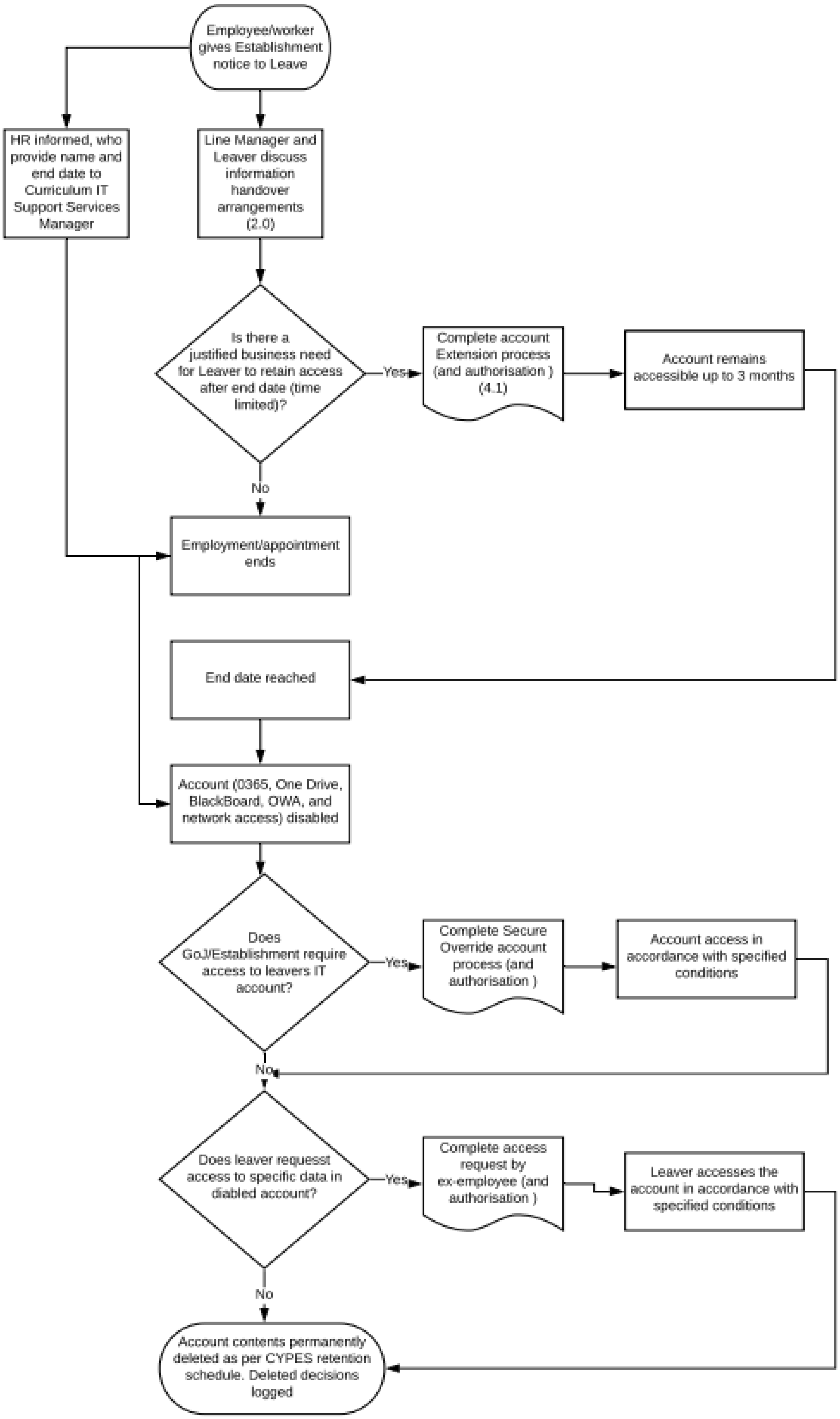
Secure account override procedure:
https://soj/depts/ModernisationAndDigital/Documents/ID%20IS%20guidelines%20for%20Cloud%20Computing%20v10%2020130328%20JB.pdf#search=secure%20account%20override

Government of Jersey ICT Equipment/Facilities Conditions of Use (for Visitors):
file://ois.gov.soj/sojdata/ESC_HomeDirs/MunnA/IT/ID%20Government%20of%20Jersey%20ICT%20Equipment%20and%20Facilities%20condition%20of%20use%20JI.pdf

Corporate records management policy:
https://soj/DocsForms/Documents/Records%20management/P%20Corporate%20Records%20Management%20Policy%20%28RM-POL-001%29%2020150622%20RY.pdf

8. Appendicies

Appendix 1: Leavers IT Arrangments Flowchart


Employee/worker gives Establishment notice to Leave
HR informed, who provide name and end date to Curriculum IT Support Services Manager
Line Manager and Leaver discuss information handover arrangements (2.0)
Is there a justified business need for Leaver to retain access after end date (time limited)?
Yes
Complete account Extension process (and authorisation) (4.1)
Account remains accessible up to 3 months
No
Employment/appointment ends
End date reached
Account (0365, One Drive, BlackBoard, OWA, and network access) disabled
Does GoJ/Establishment require access to leavers IT account?
Yes
Complete Secure Override account process (and authorisation)
Account access in accordance with specified conditions
No
Does leaver requesst access to specific data in diabled account?
Yes
Complete access request by ex-employee (and authorisation)
Leaver accesses the account in accordance with specified conditions
No
Account contents permanently deleted as per CYPES retention schedule. Deleted decisions logged

CHANGE HISTORY

Version	Date Issued	Issued by	Reason for Change
1.2.1	May 2020	Head of Governance	New document - provides overview of IT access and information security measures before and after curriculum staff leave.

Presented To	Approved by:	Date
Secondary Head Teachers		
Primary Head Teachers		
Senior Management Team		
Ministerial Team		

APPROVAL

ADDITIONAL INFORMATION

Planned review date:	**Distribution:**	
Associated policies	**Name**	**Reference**