Government of JERSEY

Children, Young People, Education and Skills

Acceptable Usage Agreement for Staff in Educational, Youth Service and Residential Care Settings

Document Purpose	To outline the appropriate use of IT equipment and platforms.
Author	CYPES Governance Team (Digital)
Publication Date	13/11/2024
Target Audience	Staff working in Education, Youth Service and Residential Care settings All other GoJ staff should refer to the Central Acceptable Use Policy
Circulation List	All CYPES staff in Education, Youth Service and Residential Childcare Settings
Description	This Acceptable Usage Agreement outlines the responsibilities and acceptable behavior expected of all staff when using any technology for work purposes, and when - communicating with students, parents, colleagues, and other stakeholders.
Linked Policies	1. *Remote - Home Working Policy (Info-Sec-Pol-013) - Information security policies* 2. *BYOD (Bring Your Own Device) Policy (Info-Sec-Pol-012) - Information security policies* 3. *CYPES Clear Desk re& Screen Policy* 4. *Information Classification Policy (Info-Sec-Pol-005) - Information security policies* 5. *RM-POL-001 – Corporate Records Management Policy - Records - Home (sharepoint.com)* 6. *Data Protection Policy (or contact dataprotection2018@gov.je)* 7. *Retention Schedules - Children, Young People, Education and Skills retention schedules (gov.je)* 8. *Individual School Policies* 9. *CYPES Data Security policy*

	10. *AI Policy - P AI In Jersey Education Policy 20231006.pdf (gov.je)* **11.** *Online Safety policy* **12.** CYPES Wi-Fi/Unknown network guidelines **13.** *CEYS – Early Years Statutory Guidance*
Approval Route	Education SLT CSC SLT COD DLT
Review Date	November 2025
Contact Details	cypesgovernance@gov.je cypesdigital@gov.je

1. Overview

This Acceptable Usage Agreement outlines the responsibilities and acceptable behaviour expected of all staff working in Education, Youth Service or Residential Care Home settings when using any technology for work purposes and when - communicating with students/children, parents/guardians, colleagues, and other stakeholders.

2. Scope

This agreement applies to:

- *All staff, including permanent, temporary, visiting employees, contractors and other 3rd parties with access to school, youth service, residential care home, government systems and technology.*
- *The use of all digital technology, Internet and electronic communication platforms (e.g., emails, learning platforms, Wi-Fi, school systems).*
- *Personal and professional usage of devices within educational, youth, residential care homes and other GoJ sites.*

3. *Monitoring*

All systems are continuously monitored and periodically audited. The purpose of this activity is to ensure that threats to systems and data are identified as early as possible to minimise impact to the business and to ensure the safeguarding of the children in our care.

*If illegal activities are detected, GoJ will inform law enforcement and regulatory agencies such as Jersey Office of the Information Commissioner (**JOIC**) as required.*

3.1. *Monitoring of user activity*

- *Tools to support safeguarding are used in all Educational, Youth Service and Residential Care Home sites, these are used to filter internet use and monitor device and internet use.*
- *GoJ detects unauthorised activity by recording what information has been accessed, by whom, and when it was attempted. GoJ needs to determine if this activity is suspicious and where necessary, prevent any further misuse or harmful effects. If the activity is violating policy requirements, action will be taken as described in Section 3 above.*
- *GoJ also has legislative requirements to be open and transparent. GoJ will seek appropriate authorisation before performing data discovery processes. These are a combination of automated and manual collection processes to satisfy the authorisation. Discovery processes will examine (but not limited to):*

- *data storage platforms (e.g., files on your computer, shared devices and Government, Education, Youth Service and Residential Care Home IT systems)*
- *collaboration platforms (e.g., Intranet sites, ticketing systems)*
- *communication platforms (e.g., emails, chat and meeting history and other messaging systems).*

3.2. *Incident Reporting*

- *If an incident occurs within a school setting*
    - *you must immediately notify the schools Data Protection Officer and follow the school guidance.*
    - *Alternatively, you may refer to your line manager.*
    - *If immediate action can be taken i.e. recovering a lost document or device, then please undertake this and document any actions.*
    - *you must report any security concerns as soon as you become aware of them. You can do this by raising a security incident via the button on the MyStates home page (https://soj)*

- *If you are outside a school setting eg a Youth site or Residential Home or are a **schools Data Protection Officer***
    - *you must report any security concerns as soon as you become aware of them. You can do this by raising a security incident via the button on the MyStates home page (https://soj)*
    - *you should engage with your Departmental Governance representative to support you (cypesgovernance@gov.je). This requirement extends from potential weaknesses to actual breaches and policy violations. CYPES will work with Departments to log and track the issue and correlate it with any similar events that occur. – For further details, please refer to the CYPES Data Security Policy.*
    - *If immediate action can be taken i.e. recovering a lost document or device, then please undertake this and document any actions.*

3.2.1. *Email archival*

- *All @gov.je and @health.gov.je emails sent and received, internally and externally, are automatically archived in a secure forensic archival system. Users should therefore be aware that all messages, even if deleted or altered in Outlook, will be retrievable for a period determined by data retention schedules and may be used to satisfy legal requirements for example Subject Access Requests (SARS) and Freedom of Information (FOI) requests. This does not supersede any Departmental email management processes.*
- *For all staff once emails are deleted, be aware they remain in your deleted folder. One removed from your deleted folder they then move to the super deleted folder where they are still recoverable. Once removed from this folder they are non-recoverable.*

3.3. *Personal use and privacy*

- *GoJ permit limited personal use of GoJ provided internet and email systems, providing that it follows this policy and does not adversely affect your work. However, you are discouraged from storing your personal data on GoJ systems.*
- *Where this is unavoidable this activity is done entirely at your own risk, and GoJ cannot be held liable for any claims arising from the unauthorised disclosure or loss of your personal data held by you in this way.*
- *Here personal data means data belonging to an individual and not the meaning under the Data Protection (Jersey) Law 2018 which is "any data relating to a data subject". The Government is not processing this data, has not recorded this information for processing or recorded it as part of a filing system.*
- *As this information is stored on GoJ systems, it will be discoverable and may be disclosed as part of eDiscovery*
- *If you logged in to M365 services on a personal device, this may be monitored.*

4. Acceptable use of Technology

4.1. Looking after School/GoJ/Youth/Residential Home-Owned equipment

The term 'equipment' includes (but is not limited to) computers, smartphones, and tablets issued to you by GoJ or by any GoJ managed School, Youth site or Residential Care Home. The equipment assigned to you must:

- be used for the purposes for which it was intended
- be protected from damage, unauthorised access and theft
- be reported immediately to the School or Central EDU IT Service Desk if lost or stolen and be reported as a Security Incident via MyStates.
- at the end of contract, any equipment must be returned to the relevant site.
- Be aware of any additional polices relating to school purchased equipment.

4.2. Preventing unauthorised access

Regardless of your role, the facilities that you work in hold information and systems that must be protected from unauthorised access. You must:

- lock your computer/tablet/smartphone when left unattended for any period of time.
- clear paperwork away if leaving your work area for any significant length of time (e.g. meetings or breaks). Please refer to the Clear Desk Policy for further details.
- return paperwork into relevant filing systems at the end of the working day.
- close windows in your vicinity.
- do not let anyone borrow your ID to gain access to restricted areas.
- challenge individuals you do not recognise and who are not wearing an ID.
- You are prohibited from plugging in any networked or storage equipment not provided to you (e.g. mobile phones, USB storage device) into school/GoJ-owned equipment.

4.3. Passwords and passphrases

Passwords are used in combination with your user ID to grant access to various services. They can also be used to protect OFFICIAL-SENSITIVE (and above) data when being shared or stored. Instead of using passwords, it is recommended for you to use a passphrase - a combination of several words together. This is easier for you to remember and more difficult to guess.

To build strong passphrases, you must:

- use a minimum of 15 characters
- combine unrelated words together.
- use symbols to separate words (e.g. full stop '.', hyphen '-')
- add additional numbers and symbols if it makes it more memorable

You must not use passphrases that:

- use a single dictionary word, in any language
- are examples used on the internet or in training materials (e.g. correct-horse-battery-staple)
- use simple keyboard patterns (e.g. qwertyuiop12345)
- use symbols that look like letters (e.g. P@ssW0rd)
- On rare occasions that you need to share a passphrase (e.g. when sharing a password protected document and need to share the password)
    - do not send the attachment/passphrase using the same technology (e.g. email)
    - send them via different methods (e.g. send by email, provide password over the phone)
    - be discrete if you are sharing passphrases via phone calls
    - delete passphrases stored electronically when no longer needed.

- If you suspect that your user account or passphrase has been compromised, change your passphrase immediately and log it via “Report a Security Incident.”

4.4. Multi Factor Authentication (MFA)

MFA MUST be enabled and utilised.

4.5. Working remotely

The need to working remotely is an identified requirement. In order to support this you may be provided with:

- portable equipment
- secure access to services from a personal device, such as access to M365.

4.5.1. Working remotely with your equipment

You may be provided with equipment that is portable and usable outside of your working location. When using this portable equipment in public, ensure that you are in complying with the Remote-Home Working Policy

For guidance on connecting to public Wi-Fi, please see CYPES Wi-Fi/Unknown network guidelines.

4.5.2. Working remotely to access specific services

When working remotely on personal devices, you must access all information via the services provided and interact via these services. You must not download a copy of this information and store it locally.

4.6. Control failure does not imply permission

The failure of security tools and controls to block certain actions should not be taken as implied permission to ignore policy requirements. You must immediately report any failures as a Security Incident via MyStates.

5. Acceptable use of communications

5.1. Use of the internet

GoJ provides access to the internet for business and education purposes. Since Government cannot guarantee the security of internet resources, you must NOT:

- download, run or install software from the internet, without permission.
- use any internet hosted storage services that are not approved (e.g. OneDrive for Work/School and Egress)
- intentionally access, download, store, process, publish, display or send media (e.g. videos, photos and audio) that are illegal, pornographic, discriminatory, hateful or likely to offend
- reproduce news articles, blogs or other external media, as they may be subject to copyright law. Obtain permission before using or circulating such media from the blog writer or media organisation
- intentionally try to access Government information or systems that you are not authorised to access

5.2. Use of email

Suspicious emails (e.g. virus warnings, security threats, offers, scams, chain emails) should not be opened, replied to or sent onto colleagues. For further guidance, search for “Phishing” on the Intranet.

Other email good practices to follow are:

- avoid sending files wherever possible; instead send a link to the file location (e.g. on SharePoint or Teams)
- avoid embedding attachments in Calendar invites, instead provide a link to the file location (e.g. on Teams or Shared drives)
- where you need to send data classified under the Information Classification Policy (Info-Sec-Pol-005) as OFFICIAL-SENSITIVE or sensitive personal data this needs to be encrypted and sent using the approved secure email solution (i.e. Egress). Please contact the Governance Team for support and guidance.
- using the “Bcc:” field rather than “Cc” when sending emails to third parties, and when communicating with many recipients
- avoid broadcasting emails to lots of people. Instead, limit the recipients to those who need to know
- convert documents to PDF when being sent externally. PDFs preserve the integrity of their contents and minimise the risks associated with sending hidden data by mistake.

You must NOT:

- sign up to websites or services with your work email address, unless required to as part of your role (e.g. procurement, training, equipment purchasing, service notifications)
- use it as a primary point of contact for your personal affairs (e.g. banking, healthcare, legal advice)
- set up a forward from your work email to a personal email address
- set up an email forward to any other person or mailbox without line manager approval

5.3. Use of voice and post

When speaking about sensitive matters, be aware of the risks of being overheard. To maintain the confidentiality of sensitive information:

- use meeting rooms or close the door of the room you are in
- use headphones when making calls from your phone or computer and ensure you are discreet when relaying sensitive information (e.g. Teams calls)

If posting or sending sensitive information by courier, ensure the package is appropriately labelled so as not to describe its contents.

5.4. Unacceptable Use

For the avoidance of doubt, the following behaviours are considered an unacceptable use of Government systems, therefore are direct violations of this policy:

- intentionally disabling or bypassing security controls
- making unauthorised copies of information, passing information to third parties without authorisation, or retaining information after your contract of employment has ended.

6. Acceptable use of information

6.1. Information classification

All information, whether electronic or paper-based, must be protected according to its sensitivity and the impact of a breach. The key principles are:

- there are three broad classification levels: OFFICIAL, SECRET and TOP-SECRET
- most of the day-to-day business of government, service delivery, commercial activity and policy development is classed as OFFICIAL
- if you need to emphasise that the artefact is for a restricted audience, add the sub-category SENSITIVE to imply these constraints are necessary, i.e. OFFICIAL–SENSITIVE eg for Safeguarding
- Where such classification has not been applied, it should be deemed OFFICAL by default

- additional protective controls may be required. Please refer to the Information Classification Policy (Info- Sec-Pol-005) for more information.

For further guidance, please email cypesgovernance@gov.je

6.2. Information handling

Your employer is the owner of all information you produce during the normal course of your employment. Therefore, you must protect the integrity of this information during its use.

When handling information, you must:

- Be aware each school is a separate Data Controller
- apply an appropriate classification label as described in Information Classification Policy (Info-Sec-Pol- 005)
- store the information securely with appropriate access controls for that classification level
- send a link to the information if it is stored internally, or a PDF copy if sent externally. The original version should be considered when first two options are unsuitable
- gain formal authorisation / data sharing agreements for sharing large quantities of data across departments, with external suppliers or other schools. Contact your Department Governance representative for support and guidance (cypesgovernance@gov.je). When considering sharing data across departments, with external suppliers or with other schools, refer to the Privacy Policy of the Data Controller.
- Data sharing must only be done with a specific purpose and lawful basis
- When the decision has been made to destroy information (please refer to your retention schedules), use confidential shredding bins or deletion.
- If using AI, data must be handled in line with the AI Policy.

6.3. Document Management

Documents created as part of your day-to-day work must be stored on:

- your department/schools document management system e.g. SharePoint
- an agreed Microsoft Teams or SharePoint site
- printed to paper (where this is required, though Government preference is to operate in a paper-lite manner) and placed in the appropriate filing system.

6.4. Retention Schedule

- All data is subject to being destroyed in accordance with the relevant data retention schedule. These can be found here: Children, Young People, Education and Skills retention schedules (gov.je)

7. Agreement

Name :

Signature:

Date :

CHANGE HISTORY

Version	Date Issued	Issued by	Reason for Change
1	13/11/24	CYPES	First Publication
1.1	05/12/24	CYPES	Amendment – Addition of 4.4 MFA
1.2	24/09/25	CYPES	Amendment – Addition to 5.2 forwarding of emails
			Update

APPROVAL

Presented To	Approval Date
Chief Office Directorate Team	11/11/23
Education Senior Leadership Team	04/11/23
CSC Department Leadership Team	30/10/24
Ministerial Team	For Note