Hautlieu School - Data Protection Policy

Author – KBL

Agreed by Staff – October 2018 Agreed by Governors – May 2020 Reviewed – September 2019 September 2020 September 2021 November 2022 November 2023 November 2025 To be reviewed by – September 2026

Introduction

Hautlieu School collects and uses certain types of personal information in relation to staff, students, parents/carers and other individuals who come into contact with the school in order to provide an education service and other associated functions. 'Personal data' means any data which relates to or identifies a living person. Within this, 'Special category data' is also a type of personal data. Essentially it is personal data which the Law considers to be more 'sensitive' and there are extra rules about how and when it can be processed, and for what purpose.

Special category data includes:

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- Trade union membership;
- Genetic or biometric data that is processed for the purpose of uniquely identifying someone;
- Data concerning health;
- Details about a person's sex life or sexual orientation;
- Data about a person's criminal record or alleged criminal activity.

In addition, Hautlieu School may be required by Jersey law to collect and use certain types of information to comply with statutory obligations of the Department for Children, Young People, Education and Skills, and share this information with other organisations. Please see our Privacy Statement in Appendix A or on the school website for further details.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection (Jersey) 2018 Law and other related legislation, and is designed to protect the privacy of individuals and bring equivalence with the obligations brought to bear by the European GDPR (General Data Protection Regulation). It

will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Responsibilities

The Department for Children, Young People, Education and Skills have provided to schools a comprehensive Data Protection Policy 2006ESCPolicyTemplate.doc and provide general guidance to schools, parents and staff in relation to when dealing with personal information in their daily work.

The complete Government of Jersey guide to data protection legislation can be found at Children, Young People, Education and Skills privacy policy

Under the Data Protection (Jersey) 2018 Law, schools are classed as separate entities, known as "Data Controllers", rather than as a collective part of the Department for Children, Young People, Education and Skills, or Government of Jersey. As such, Hautlieu School is classified as a Data Controller and registered with the Jersey Office of the Information Commissioner (No 16495).

Each establishment and its employees must comply with the Data Protection Principles and other requirements of the Law. Staff must be fully familiar with this Data Protection Policy and the Department of Children, Young People, Education and Skills Data Protection Policy, and carefully follow the advice given to Hautlieu Staff. Staff are reminded that they have a legal obligation to protect the information that we hold on students and staff.

2. **Data Protection Principles.**

Staff are required to adhere to the principles of data protection as laid down by the Law at all times. In accordance with those principles personal data shall be:

1. "lawfulness, fairness and transparency"
   processed lawfully, fairly and in a transparent manner
2. "purpose limitation"
   collected for specified, explicit and legitimate purposes (and not used for an incompatible purpose);
3. "data minimization"
   adequate, relevant and limited to what is necessary
4. "accuracy"
   accurate, kept up to date (erasing or rectifying inaccurate data without delay)
5. "storage limitation"
   kept for no longer than is necessary for the purposes; and
6. "integrity and confidentiality"
   Ensure appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (using appropriate technical or organisational measures).

3. **Our Commitment**

Hautlieu School is committed to maintaining these data protection principles at all times.

This means that the school will:

- Tell parents/carers what purposes we will use student information for when we collect it. Please see the attached Hautlieu School Privacy Notice (Appendix A)

- Tell staff what purposes we will use staff personal information for when we collect it. Please see attached Hautlieu School Privacy Notice (Appendix A)
- If information will be shared with third parties we will inform parents /carers / individual staff of the reasons why, with whom and under what circumstances
- Check annually the quality and accuracy of the information we hold
- Apply our records management procedures to ensure that information is not held longer than is necessary
- Ensure that when information is authorised for disposal it is done appropriately (Shredding)
- Ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on our computer system (SIMS)
- Only share personal information with others when it is necessary and legally appropriate to do so
- Set out clear procedures for responding to requests for access to personal information known as subject access requests in the Data Protection Act (Appendix B)
- Appoint a Data Protection Officer as required by Article 24 of the Data Protection (Jersey) 2018 Law
- Train our staff so that they are aware of our and the Department of Children, Young People, Education and Skills policies and procedures
- This policy will be continually reviewed and updated to reflect changes in our services and feedback from service users, as well as to comply with changes in the law

The Data Protection Officer will:

- Inform and advise the school and all members of the school community of their obligations under the Law
- Monitor compliance with the Law in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits
- Provide advice where requested as regards data protection impact assessments and monitoring the process covered by it
- Have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing
- Respond quickly to any queries regarding data protection, including subject access requests and complaints
- Liaise with the Data Protection Team and/or the Corporate Protection Officer as required
- Swiftly bring any data protection breaches to the attention of the Data Protection Team (breach@gov.je) and support the team as instructed in resolving breaches

All staff will ensure that:

- Personal data is processed only in accordance with the Data Protection (Jersey) Law 2018
- all personal data is kept securely
- Work related emails are not forwarded to personal email addresses
- They are aware of online safety issues and promptly share any concerns about staff and/or students to the Designated Safeguarding Lead as outlined in the Hautlieu School Safeguarding Policy
- No personal data is disclosed either verbally or in writing, to any unauthorised third party
- Personal data is kept in accordance with the Government of Jersey and Hautlieu retention schedules
- Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Protection Officer for advice
- Any data protection breaches are swiftly brought to the attention of the Data Protection Officer and that they support them as instructed in resolving breaches

- The Data Protection Officer is involved, properly and in a timely manner, in all issues that relate to the protection of personal data
- Any visitors, contractors, short-term or voluntary staff are informed of the details of this policy and their requirement to comply with it, and that all practical and reasonable steps are taken to ensure that these staff do not have access to any personal data beyond what is essential for the work to be completed

4. **Complaints – Failure to comply with Data protection Responsibilities**

As outlined in the Hautlieu School Fair Processing Statement, complaints under this policy should be made to the School Data Protection Officer. Alternatively, complaints can also be made to the Information Commissioner's Office in Jersey.

Links to UN Convention on the Rights of the Child

- Article 16: You have the right to a private life. For instance, you can keep a diary that other people are not allowed to see

Responsibilities
• Monitoring – School Data Protection Officer • Evaluating – SLG • Policy Overview – SLG and Governors • Circulation – All staff

Minor revision history – reason and date
KBL – Changed States to Government of Jersey, September 2019
KBL – Added in links to the UN Convention on the Rights of the Child
KBL – Changed Social Security for Customer and Local Services, September 2019
KBL – Changed Education Department to Children, Young People, Education and Skills, September 2019
KBL – Updated Appendix A; Organisations that Process Data, September 2019
KBL – Updated Appendix C; Staff Acceptable Use Policy Clause (a), September 2019
KBL – Updated Appendix A; postal address for Information Commissioner's Office, September 2020
KBL – Updated A; Organisations that Process Data, September 2020
KBL – Updated Privacy Notice and Appendix B to include Contact Tracing, September 2021
RSM – Updated Privacy notice Sept 2023
RSM – Policy reviewed and updated links Nov 2023
RSM – Updated Hautlieu acceptable use policy (students) May 2025
RSM – Implemented CYPES acceptable use policy (staff) Sept 2025

Appendix A

Hautlieu School Jersey

Privacy Notice 2025

Hautlieu School Jersey is registered as a 'Controller' under the Data Protection (Jersey) Law 2018 as we collect and process personal information about you. We process and hold your information in order to provide public services and meet our statutory obligations. This notice explains how we use and share your information. Information may be collected on a paper or online form, by telephone, email, or by a member of our staff, or in some cases, by another Government department.

We will continually review and update this privacy notice to reflect changes in our services and feedback from service users, as well as to comply with changes in the law.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but it is not restricted to:

- Date of Birth, gender and identification documents
- Contact details and contact preferences
- Parental Responsibility
- Student and curricular records including attendance information
- Results of internal assessments and externally set tests and exams
- Safeguarding information
- Exclusion information
- Photographs
- CCTV images captured in school
- Details of positive cases of Covid-19 in the school community

We also collect, store and use information about you that falls into 'special categories' of more sensitive personal data. This includes information about:

- Characteristics such as ethnicity, languages spoken and eligibility for certain benefits including the Jersey Premium
- Family circumstances
- Physical and mental health, including medical conditions
- Support received including care packages, plans and support providers
- Biometric Data

We may also hold data about you that we have received from other organisations, including other schools and the Government of Jersey Customer and Local Services Department.

Why we use this data

We need to collect, use and hold this data in order to:

- Stay in touch with you, answer your queries and provide you with the information that you need including with regard to the running of the school (such as emergency closures) and events

- Verify you are who you say you are and safeguard all members of the Hautlieu School Community
- Handle your applications
- Meet our statutory obligations including to support student learning, monitor and report on student progress and provide appropriate pastoral care
- Carry out the service we provide, and to monitor and improve our performance in responding to your service requests
- Ensure that we meet our legal obligations and, where necessary, for law enforcement functions
- Prevent and detect crime
- Where necessary, protect individuals from harm or injury including anything that may endanger an individuals' health
- Allow the statistical analysis of data so we can plan the provision of services
- Comply with the law regarding data sharing

How we will use this information about you

We will use the information you provide in a manner that conforms to the Data Protection (Jersey) Law 2018.

We will endeavour to keep your information accurate and up to date and not keep it for longer than is necessary. In some instances the law sets the length of time information has to be kept. Please ask to see the States of Jersey Department for Children, Young People, Education and Skills retention schedules for more detail about how long we retain your information.

We may not be able to provide you with a service unless we have enough information or your permission to use that information.

We will not pass any personal data on to anyone outside of the Government of Jersey, other than those who either process information on our behalf, or because of a legal or statutory requirement, and we will only do so, where possible, after we have ensured that sufficient steps have been taken by the recipient to protect your personal data.

We will not disclose any information that you provide 'in confidence', to anyone else without your permission, except in the few situations where disclosure is required by law, or where we have good reason to believe that failing to share the information would put someone else at risk. You will be told about this unless there are exceptional reasons not to do so.

We upload students' data to the SIMS database that is hosted in the European Union which is shared with the Government of Jersey Department for Children, Young People, Education and Skills. We also use a number of web-based applications as part of our teaching, tracking and monitoring of students in order to support them in achieving their very best. Applications such as Go4Schools and Kerboodle (for example) require us to share personal information with them in order to make effective use of the facilities they offer to support students in their learning. Decisions on using these applications are carefully considered and a thorough due diligence process is followed as to how companies hold and use the data to check their suitability.

In addition, students' data may be uploaded to GL Assessments, ALPS, examination boards and a small amount of personal data is also stored (name, email address) on the Dynamic Learning database as well as for the SIMs InTouch service. All of these services are hosted

within the European Union. To understand how this information is processed in more detail please see Appendix A.

Furthermore, please note that CCTV is only captured in an overt way with clear and visible notices declaring the cameras presence and use on the school site. Images are kept for 30 days in a secure location and are only viewed when necessary to safeguard all those persons accessing the Hautlieu site.

Data Sharing

As a school we are required to pass on data to The Department for Children, Young People, Education and Skills. When a student is transferring to another school or college, Hautlieu School and / or the Department for Children, Young People, Education and Skills will pass on all information relevant to the education and care of the student to the other institution, in accordance with our public function. Information is also passed to UK examination and assessment organisations for processing. The resultant information is returned to both schools and the Department for Children, Young People, Education and Skills. If your son or daughter is shortly to leave their current school, and to ensure their continuing education and care, details held in their files will be passed on to Hautlieu School. The Department for Children, Young People, Education and Skills also uses the information to derive statistics to inform decisions on (for example) the funding of schools, and to assess the performance of schools and set targets for them. The statistics are used in such a way that the individual students cannot be identified from them.

We may need to pass your information to other Government of Jersey departments or organisations to fulfil your request for a service such as Health, Children's Social Care, and Customer and Local Services. These departments and organisations are obliged to keep your details securely, and only use your information for the purposes of processing our service request. Please read Appendix B for a list of organisations your data is shared with and how.

We may disclose information to other departments where it is necessary, either to comply with a legal obligation, or where permitted under other legislation. Examples of this include, but are not limited to: where the disclosure is necessary for the purposes of the prevention and/or detection of crime; for the purposes of meeting statutory obligations; or to prevent risk of harm to an individual.

At no time will your information be passed to organisations for marketing or sales purposes or for any commercial use without your prior express consent.

We will also be required by law to publicise certain information, for example performance data, but in these instances you data will be anonymised to protect your identity. We will not publish any of your sensitive personal information unless there is a requirement for us to do so in order to carry out our statutory functions.

Communicating with us

If you email us we may keep a record of your email address and a copy of the email for record keeping purposes.

For security reasons we will not include any confidential information about you in any email we send to you. We would also suggest that you keep the amount of confidential information you send to us via email to a minimum or correspond with us by post.

We will not share your email address or your email contents unless is it necessary for us to do so either to fulfil your request for a service, to comply with a legal obligation, or where permitted under other legislation.

We do not record or monitor any telephone calls you make to us using recording equipment, although if you leave a message on our voicemail systems your message will be kept until we are able to return your call or make a note of your message. File notes of when and why you called may be taken for record keeping purposes. We will not pass on the content of your telephone calls, unless is it necessary for us to do so either to fulfil your request for a service, to comply with a legal obligation, or where permitted under other legislation.

Your rights

You can ask us to stop processing your information

You have the right to request that we stop processing your personal data in relation to any of our services. However, this may cause delays or prevent us delivering a service to you. Where possible we will seek to comply with your request but we may be required to hold or process information to comply with a legal requirement.

You can withdraw your consent to the processing of your information

In the few instances when you have given your consent to process your information, you have the right to withdraw your consent to the further processing of your personal data. However, this may cause delays or prevent us delivering a service to you. We will always seek to comply with your request but we may be required to hold or process your information in order to comply with a legal requirement.

You can ask us to correct or amend your information

You have the right to challenge the accuracy of the information we hold about you and request that it is corrected where necessary. We will seek to ensure that corrections are made not only to the data that we hold but also any data held by other organisations/parties that process data on our behalf.

You can request that the processing of your personal data is restricted

You have the right to request that we restrict the processing of your personal information. You can exercise this right in instances where you believe the information being processed in inaccurate, out of date, or there are no legitimate grounds for the processing. We will always seek to comply with your request but we may be required to continue to process your information in order to comply with a legal requirement.

You can ask us for a copy of the information we hold about you

You are legally entitled to request a list of, or a copy of any information that we hold about you by completing a subject access request. However, where our records are not held in a way that easily identifies you, we may not be able to provide you with a copy of your information, although we will do everything we can to comply with your request.

Complaints

If you have an enquiry or concern regarding the processing of your personal data please contact our Data Protection Officer Ros Martin (Deputy Headteacher) on telephone: 01534 736242 or at r.martin@hautlieu.sch.je or write to Hautlieu School, Wellington Hill, St Saviour, Jersey JE2 7TH.

Alternatively, you can make a complaint to the Information Commissioner's Office on telephone 01534 716530 or at enquiries@jerseyoic.org or write to Office of the Information Commissioner, 2nd Floor, 5 Castle Street, St Helier, Jersey, JE2 3BT.

Hautlieu School Jersey

Organisations that Process Data

Hautlieu School Jersey is registered as a 'Controller' under the Data Protection (Jersey) Law 2018 as we collect and process personal information about you. We process and hold your information in order to provide public services and meet our statutory obligations. Our Privacy notice explains how we use and share your information.

Hautlieu School Jersey process data utilising or have an agreement with the following organisations:

- SIMS in order to hold a student record file, for statutory obligations and to ensure that we meet our legal obligations, to track and monitor a student's academic and pastoral progress, and to provide you with the information that you need
- GL Assessments for statutory obligations including tracking and monitoring student progress
- ALPs to track and monitor student, department and school achievements and progress
- Joint Council for Qualifications and Examining Boards including AQA, OCR, Pearson, CIE, WJEC, TQUK and HSK for statutory obligations including providing examination information for students to be able to collect their examination results in addition to tracking and monitoring examination progress
- My Concern for statutory obligations and to ensure that we meet our legal obligations to safeguard all students and members of the Hautlieu Community
- Show My Homework, Dynamic Learning, the Open University and Cambridge Elevate in order to utilise appropriate online teaching and learning tools, for statutory obligations within teaching and for tracking and monitoring of students learning
- Parent Mail and In Touch in order to communicate effectively with you, to provide you with information you need, to carry out a service you have requested, and to monitor and improve our performance in responding to your service request
- School Cloud in order to communicate effectively with you with regard to booking parents evening appointments
- Go4Schools in order to meet statutory obligations within teaching and for tracking and monitoring of students learning
- 1 &1 Web Hosting, Office 365 and Keybr in order to utilise appropriate online teaching and learning tools and for statutory obligations within teaching
- Adobe Acrobat in order to meet our statutory obligations with regard to teaching and learning
- Hogg Robinson Group to carry out a service you have requested in relation to a school trip or course and comply with financial directions
- Iris Connect where recordings of lessons are uploaded and shared with select groups in order to meet our statutory obligations and provide training opportunities for staff to improve teaching and learning

- Isaac Physics, Zig Zag Education - E Revision, The Resilience Development Company and Tassomai in order to utilise appropriate online teaching and learning tools, in order to track and monitor student progress
- Unifrog in order to meet our statutory obligations and provide careers advice and guidance to students
- Dr Frost Maths, Complete Maths TUTOR and Kerboodle in order to support, track and monitor student progress
- UCAS in order to meet our statutory obligations and support students in their applications for Higher Education
- Applicaa, in order to process applications for a school place at Hautlieu
-

We will continually review and update our sharing agreements to reflect changes in our services and feedback from service users, as well as to comply with changes in the law.

Hautlieu School Jersey

Data Sharing with Organisations

Hautlieu School Jersey is registered as a 'Controller' under the Data Protection (Jersey) Law 2018 as we collect and process personal information about you. We process and hold your information in order to provide public services and meet our statutory obligations. Our Privacy notice explains how we use and share your information.

Hautlieu School Jersey shares data with the following organisations:

- Departments within the Government of Jersey for statutory obligations, verification purposes, to provide you with the information you need, to answer your query, to allow the statistical analysis of data so we can plan the provision of services and to ensure that we meet our legal obligations
- The Police in order to prevent and detect crime, for statutory obligations, where necessary to protect individuals from harm or injury and where necessary for our law enforcement functions
- The Fire Service for statutory obligations around staff training
- Health Services including CAMHS, MASH, MARAC and JMAPPA for statutory obligations, to ensure that we meet our legal obligations, where necessary to protect individuals from harm or injury and to provide you with the information that you need
- Social Services for statutory obligations, to ensure that we meet our legal obligations, where necessary to protect individuals from harm or injury, to provide you with information you need, to carry out the service you have requested, and to monitor and improve our performance in responding to your service request;
- Customer and Local Services to provide you with information you need, carry out the service you have requested, and to monitor and improve our performance in responding to your service request
- Other Schools and Colleges in order to meet our statutory obligations, to provide you with the information you need, and to meet our legal obligations

We will continually review and update our sharing agreements to reflect changes in our services and feedback from service users, as well as to comply with changes in the law.

Appendix B

Procedures for Responding to Subject Access Requests for Personal Information in Accordance with the Data Protection (Jersey) Law 2018

Anybody who makes a request to see their file or their son / daughters file or other personal data held on them is making a request under the Data Protection (Jersey) Law 2018.

The Data Protection (Jersey) Law 2018 provides individuals with a right to access personal data which is processed about them by a data controller, such as Hautlieu School. Individuals are entitled to be informed:

- Whether their personal data is being processed by the school (or on the school's behalf)
- The purposes for which they are being or are to be processed by or on behalf of that controller;
- The categories of personal data concerned
- The recipients or classes of recipients to whom they are or may be disclosed
- How long that data is likely to be retained
- Where the data was collected from if not from them
- About any automated decision making about their personal data and the rationale behind it
- About safeguards in place where data is transferred to a third country (this usually means outside Europe) or international organisation

Individuals also have rights to:

- Lodge a complaint with the Data Protection Authority
- Request rectification, erasure, restriction of processing (under certain circumstances)
- Object to processing on the basis of direct marketing, legitimate interest or public function
- Request for their data to be provided in a structured machine readable format in order to transmit to another data controller (portability)

Crucially, individuals can also ask, free of charge, for a copy of personal data processed about them by Hautlieu School and this must be (with some exceptions) provided within four weeks.

This right of access includes both electronic records and paper records. Hautlieu School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within the 4 week limit set out in the Data Protection (Jersey) Law 2018.

Individuals will not be entitled to access information to which any of the exemptions in the Law applies. However, only those specific pieces of information to which the exemption applies will be withheld and determining the application of exemptions will be made by the SAR Point of Contact in the Department for Children, Young People, Education and Skills. In the event of any uncertainty around exemptions, the final decision will be made by the Data Protection Team under the guidance of the CDPO as required.

Hautlieu School is no longer permitted by Law to charge a fee to complete a subject access request, although an administrative charge can be made for extra copies.

Any individual wishing to exercise this right should access the online portal at https://www.gov.je/Government/dataprotection/SubjectAccessRequests/Pages/SubjectAccessRequest.aspx where they will be directed to an online form.

Appendix C

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 behaviour 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)

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 :