Government of JERSEY

Children, Young People, Education and Skills

Data Protection Policy

Document Purpose	Policy
Author	CYPES Governance Team
Publication Date	July 2025
Target Audience	All CYPES Staff: Permanent, temporary, and part-time employees.
Circulation List	All CYPES Staff: Permanent, temporary, and part-time employees.
Description	This Data Protection Policy is designed to give CYPES staff clear instructions regarding their obligations for the collection, use, storage and sharing of personal information.
Linked Policies	Data Protection (Jersey) Law 2018 Children, Young People, Education and Skills privacy policy Data Security Policy.pdf Data Sharing Policy.pdf Data Retention Policy.pdf Easy reference Guide for Breach process as per the Privacy Framework 2022.pdf
Approval Route	CYPES Ministerial Team CYPES DLT CSC SMT
Review Date	July 2028
Contact Details	cypesgovernance@gov.je

1. Overview

The processing of personal data is essential to many of the services and functions carried out by the Department for Children, Young People, Education and Skills (CYPES), and this policy sets out how CYPES complies with the Data Protection (Jersey) Law 2018 and other related legislation.

Adherence to the legislations reduces the likelihood of an information security breach and its wider effects, including causing harm or distress to data subjects, and reputational damage to the Department.

Since the delivery of many of CYPES services and functions are reliant on the processing of accurate and useable personal data, adherence to the legislation will improve efficiency and effectiveness in the public interest and maintain the trust of data subjects and service users.

2. Scope

This policy applies to all CYPES employees:

- All CYPES staff: Permanent, temporary, and part-time employees.
- Contractors and Consultants: Any third-party individuals or organisations providing services to CYPES.
- Volunteers and Interns: Individuals engaged in unpaid work or training with CYPES.
- Partner Organisations: External entities that collaborate with CYPES and access its information.
- Service Providers: Vendors and service providers or any data processor who processes data on behalf of CYPES.

3. Responsibilities and distribution

Government of Jersey – Are responsible for ensuring that the use of personal and sensitive data is compliant with the Data Protection (Jersey) Law 2018.

Employees – Have the responsibility to comply with the law by following data protection policies and procedures, as well as reporting concerns and breaches.

All levels of management – Are responsible for ensuring their staff are kept up to date with relevant policies, training and procedures and adhere to them.

4. Policy/Standards

What is Data Processing

Data processing means “any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.

It is a very broad definition. Any data you handle is likely to fall within this definition.

Principles of Data Protection
In accordance with the principles of the Data Protection (Jersey) Law 2018, the following key principles underpin this policy statement, and CYPES will comply with them by putting in place measures to ensure that personal data is:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject. **(Lawfulness, fairness and transparency)**
- Collected and created for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. **(Purpose limitation)**
- Adequate, relevant and limited to what is necessary in relation to those purposes. **(Data minimisation)**
- Accurate and, where necessary, kept up to date. **(Accuracy)**
- Retained for no longer than is necessary. **(Storage limitation)**
- Kept safe from unauthorised access, accidental loss or deliberate destruction. **(Integrity and confidentiality)**

And

- CYPES can demonstrate that it has done so **(Accountability)**

To maintain these principles CYPES will:

- Let data subjects know how and for what purpose their personal data is being processed by means of a published Privacy Notice.
- Inform data subjects if their personal data will be shared and why and with whom when there is a legitimate purpose for doing so.
- Only process personal data where there is a lawful basis to do so.
- Only re-use personal data where there is a valid reason or basis for doing so. Where the new use has been assessed as being compatible with the original purpose for which the data was provided or where specific consent has been provided.
- Check the quality and accuracy of the information it holds and make it easy for data subjects to do so.
- Ensure that information is not held for longer than necessary and that such information is destroyed appropriately and securely.
- Have safeguards in place to protect personal information in all formats from loss, theft or unauthorised disclosure.

Lawful Basis for Processing
The grounds for processing personal data are:

- **Public Function** – The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

- **Consent** – The individual has given clear consent for you to process their personal data for a specific purpose.
- **Legal obligation** – To comply with CYPES legal obligations set out in law.

There is no single basis that is better or more important than others, all are equally valid; when choosing which to rely on, the most appropriate basis to use depends on the purpose for which the data is being processed and the relationship with the individual.

To fulfil our statutory responsibilities, in most cases the lawful basis for processing personal data will be to perform a task carried out in the public interest and to comply with legal obligations set out in law.

CYPES will only ask for consent if consent is the only lawful basis for the purpose of the processing of personal information and if it is not doing so under one of the other legal basis for processing:

- **Informed Consent** - This requires that we are properly informing the data subjects of all the possible outcomes and get their consent before processing. The goal of Informed Consent is to let the data subject know all there is to know about a specific situation and allow them to decide based on that information.

- **Explicit Consent** - This means that the data subject is given the option to authorise obtaining, using, or selling of their data. This means that the data subject knows they are being asked to use or share their personal information, and they agree to it. We must make sure that we disclose the purpose for which the data will be collected and used.

- **Public Function** - To rely on Public Function as your lawful basis, the information you intend to share must be necessary to fulfil one of the following functions:

    - Meeting a health or development need.
    - Safeguarding welfare.
    - Corporate Parenting to meet a health or development need or to safeguard welfare.

- **Legal Obligation** - you can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation

Third-Party Processors
CYPES still has a legal responsibility as the data controller for data when third parties are processing it. No department or member of staff shall enter into any contract or informal data sharing agreement either online or in person with a third party unless the correct procedures have been followed. To be clear, the clicking ‘yes’ to terms and conditions on a web-based service, or raising a purchase order, are all forms of a contract.

If there is any doubt, you must seek advice from your CYPES Data Governance Officer (DGO) cypesgovernance@gov.je.

Managers who employ contractors, short term or voluntary staff must ensure they are appropriately vetted for the data they will be processing. In addition, Senior Managers and/or designated person should ensure that:

- Any data collected or processed in the course of work undertaken is kept securely and confidentially.
- All data is returned to the Department on completion of the work, including any copies that may have been made. Alternatively, the data is securely destroyed and CYPES receives notification/proof in this regard when requested.
- The Department receives prior notification of any disclosure of data to any other organisation or any other person who is not a direct employee of the contractor.
- Any data made available by CYPES or collected in the course of work, is neither stored nor processed outside of the EEA unless an agreement has been made to do so from CYPES Governance Team.
- All practical and reasonable steps are taken to ensure that contractors, short term, or voluntary staff do not have access to any data that is beyond what is essential for the work to be completed.
- Confirmation of confidentiality obligations for all employees who will access or engage with data that is being processed.

Data Security

As an integral part of the Government of Jersey, CYPES is committed to maintaining the highest standards of data security to safeguard the interests of children, young people, and the wider community.

Every staff member has a vital role in this effort. By adhering to the guidelines and procedures detailed in the attached policy, we collectively contribute to a secure and trustworthy environment for the data we manage.

Data Security Policy.pdf

Data Retention

Ensuring that CYPES erase or anonymise personal data when it is no longer needed will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. Apart from helping CYPES comply with the data minimisation and accuracy principles, this also reduces the risk that we will use such data in error.

CYPES has a statutory responsibility to respond to subject access requests for personal data, this may be unlawful if we are holding old data for longer than is necessary.

For more detail about CYPES Retention Schedules, please follow this link:
Children, Young People, Education and Skills retention schedules

Data Subjects Rights

Every individual is entitled to have their personal information protected, used in a fair and legal way, and made available to them when they ask for a copy. If an individual feels that their personal information is wrong, they are entitled to ask for that to be information to be corrected.

Data subjects rights are as follows:

- **Right to be Informed**
- **Right of Subject Access**
- **Right to Rectification**
- **Right to Erasure**
- **Right to Restriction of Processing**
- **Right to Data Portability**
- **Right to Object to Processing**

More detail can be found within the Data Protection (Jersey) Law 2018 (jerseylaw.je)

Subject Access Request

The Data Protection (Jersey) Law 2018 provides individuals with a right to access personal data which is processed about them by a data controller. It is their data and in most cases the subject can request access to anything we process on data subjects.

Individuals are entitled to be informed:

- Whether their personal data is being processed by CYPES and/or the Government of Jersey.
- The purposes for which they are being, or are to be processed by, or on behalf of CYPES and/or the Government of Jersey.
- The categories of personal data concerned.
- How long the data is likely to be retained for.
- 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 the right to:
  - Lodge a complaint with the Data Protection Authority (JOIC).
  - Request rectification, erasure, restriction of processing

- Object to processing based on 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)

Freedom of Information Request (FOI)

Freedom of Information (FOI) is legislation that gives anyone, anywhere in the world, the right to obtain information held by public authorities. Under FOI law, anyone has equal rights to access information that we, as a government, hold about almost anything.

When a FOI request is made:

- Someone asking for information does not have to say why they want it.
- We are legally obliged to provide the information, if we have it.
- We must provide the information within 20 days of the request.

FOI requires us all to organise our information so that we can respond to information requests promptly. CYPES Governance Team manages the process to manage FOIs received by the department.

Further information about Freedom of Information requests can be found here: Freedom of Information (FOI)

Data Breach Management

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, data transmitted, stored, or otherwise processed; Where a data breach occurs, or is suspected, it should be reported immediately to your Line Manager and then report using this security incident reporting tool. Report a security incident.

Follow this link to see how to manage a data breach:
Easy reference Guide for Breach process as per the Privacy Framework 2022.pdf

Training and Awareness

The human factor is crucial in preventing security incidents. Employee training, awareness and compliance are among the most critical components of an effective data protection strategy.

Since the main purpose of any data protection training program is to improve awareness and behaviour among employees, discussing employee responsibilities and best practices is integral to the program's success.

Employees have several roles and responsibilities in ensuring data protection and privacy:

- **Adhere to security policies and procedures** – Employees must become familiar with our data protection policies, either during the onboarding process or via dedicated data protection training and educational sessions.
- **Complete mandatory training** – Corporate and mandatory training is rolled out annually, when notification is received regarding any training is outstanding, treat this as urgent.
- **Attend any bespoke training programs** – Actively participate in all required data protection training sessions, whether in person or online, to understand the laws, policies, procedures that govern data protection.
- **Understand Regulations and Policies** – Employees must familiarise themselves with the relevant data protection regulations, such as the Data Protection (Jersey) Law 2018 and the Children and Young People (Jersey) Law 2022 and our organisational policies and procedures.
- **Application of best practices** – Employees are responsible for applying the data protection practices they learn during training and that are written into policies.
- **Handling personal data correctly** – Employees must follow proper procedures for handling personal and sensitive data, ensuring they collect, store, and process it only for legitimate purposes.
- **Reporting data breaches** – Employees are required to promptly report any data breaches or suspected security incidents as soon as they become aware.
- **Maintaining confidentiality** – Employees must ensure that they maintain the confidentiality of any personal or sensitive information they have access to and avoid unauthorised disclosure.
- **Updating knowledge** – Employees must keep their knowledge of data protection up to date by attending refresher courses and staying informed of changes in relevant laws or company policies.
- **Raising awareness** – Employees can also help raise awareness by encouraging their colleagues to follow best practices and share insights gained from training.

When CYPES monitoring identifies non-compliance with statutory, policy or professional requirements, appropriate actions will be identified and implemented. These actions will be recorded and communicated to the relevant employees. Non-compliance to mandatory and statutory training may result in disciplinary action and may be reported to the appropriate regulatory body.

By fulfilling these responsibilities, we contribute to a culture of compliance and help protect both CYPES and individuals' personal data.

CHANGE HISTORY

Version	Date Issued	Issued by	Reason for Change
0.1	July 2025	CYPES Governance Team	First Publication
			Review
			Update

APPROVAL

Presented To	Approval Date
CYPES Ministerial Team	4 July 2025
CYPES Departmental Leadership Teams	16 June 2025