Jèrriais Teaching Service
Data Protection Policy

As a data 'Controller' the Jèrriais Teaching Service intends to comply fully with the requirements and principles of the Data Protection (Jersey) Law 2018. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities within these guidelines.

Enquiries and Point of Contact
General information about the Data Protection (Jersey) Law can be obtained from the Office of the Information Commissioner online at www.oicjersey.org. Any concerns about security of data collected and processed by the Jèrriais Teaching Service should be brought to the attention of Marianne Sargent.

Controller
The natural or legal person, public authority, agency or other body that, whether alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor
An organisation which the Controller has commissioned to process data for a specific purpose on their behalf. The Controller is primarily responsible for the actions of the Processor.

Personal Data
Any information relating to an identified or identifiable natural person (Data Subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, identification number or location.

Sensitive Personal Data
This is now known as 'special category data' and is personal data that reveals information about a Data Subject, such as racial or ethic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, data concerning the health, sex life or sexual orientation.

Consent
In relation to the processing of a Data Subject's personal data, means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, whether orally or in writing, signifies agreement to the processing of that data.

Data Subject Rights

All Data Subjects have a right of access to their own personal data, including those listed below:

- Right to be informed (fair processing / privacy notices)
- Right of access (subject access requests)
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Right in relation to automated decision making and profiling

In order to ensure that individuals receive only information about themselves, it is essential that a formal system of requests is in place. Where a request for subject access is received, the Jèrriais Teaching Service policy is:

- Anyone with parental responsibility can make a request for information about their own child. (See the Department for Children, Young People, Education and Skills guidance with regard to 'parental responsibility'.)
- Requests from children who can demonstrate an understanding of the nature of their request will be processed as any subject access request as outlined below and the copy will be given directly to the children. (See the Department for Children, Young People, Education and Skills guidance with regard to 'age of reason'.)
- Requests from children who do not understand the nature of the request will be referred to the children's parents.
- Data will be sent in a sealed envelope to the requesting Data Subject or parent.
- Some information may have to be redacted. (See the Department for Children, Young People, Education and Skills guidance with regard to 'subject access requests'.)

In general the Jèrriais Teaching Service will only disclose data about individuals with their consent. However, there are circumstances under which the Jèrriais Teaching Service may have to reveal data without express consent. Examples of this include, but are not limited to:

- meeting statutory obligations;
- vital interest/emergency situations;
- safeguarding in order to prevent risk of harm and protect children's health, safety and welfare;
- preventing or investigating a crime;
- complying with a court order or summons that compels the Jèrriais Teaching Service to release the information.

Only authorised and properly instructed staff are allowed to make external disclosures of personal data.

The Data Protection Principles

Principle One: Lawful, Fair and Transparent
The Jèrriais Teaching Service undertakes to obtain and process personal data fairly and lawfully by informing all Data Subjects of the reasons for data collection, the purposes for which the data is held, the likely recipients of the data and the Data Subjects' rights of access. Information about the use of personal data is printed on the specific data collection documents. If details are given verbally the person collecting the data will explain the issues before obtaining the information.

Principle Two: Specified, Explicit and Legitimate Purpose
Specified purposes for the collection of data are stated on the Jèrriais Teaching Service Privacy Notice and specific data collection documents. Information held for these stated purposes will not be used for any other purpose without the Data Subjects' consent.

Principle Three: Adequate, Relevant and Limited to what is Necessary
Data held about individuals will be adequate, relevant and limited to what is necessary to the purpose of holding the data. In order to ensure compliance with this principle the Jèrriais teaching team will check records regularly for missing, irrelevant or seemingly excessive information and may contact Data Subjects to verify certain items of data.

Principle Four: Accurate and Up-to-date
Data held will be as accurate and up-to-date as is reasonably possible. If a Data Subject informs the Jèrriais Teaching Service of a change of circumstances, their record will be updated as soon as is practicable. The Jèrriais Teaching Service will send out data collection forms on a regular basis to give Data Subjects the opportunity to update their information. Data collection forms will include a statement requiring Data Subjects to inform The Jèrriais Teaching Service of any change to the information provided.

Principle Five: Not Kept Longer than Necessary
Data held about individuals will not be kept for longer than necessary for the purposes registered. However, it is important to keep data where there is a genuine need to process it, or statutory requirement to do so. The Jèrriais Teaching Service has a regularly updated retention schedule in order to keep track of the data collected. It is the responsibility of all members of the Jèrriais teaching team to ensure obsolete data is properly erased, while data that needs to be retained is stored or archived securely.

Principle Six: Data should be secure
The Jèrriais Teaching Service undertakes to ensure security of personal data by the following general methods:

- Appropriate office security measures are in place such as a lockable office door and the use of lockable filing cabinets for housing personal data collected on paper. Paper printouts and source documents are always shredded before disposal.
- The Jèrriais Teaching Service has a clear desk policy, whereby no personal data is left unattended and on show.
- Any files containing personal data stored on individual staff laptops are password protected. Otherwise personal data is stored on a central networked password protected computer within the office of the Jèrriais Teaching Service. This computer is maintained by the IT department within Children, Young People, Education and Skills, including the installation and updating of security software. Only authorised users are allowed access to the computer files and password changes are regularly undertaken.
- Before being given access to a computer staff are properly checked and sign a confidentiality agreement. All staff are instructed in their data protection obligations and their knowledge is updated as necessary.
- If personal data must be sent via email, it is done so using a password protected document and the password is sent separately using an alternative means.
- Any personal data that is taken off-site is carried in a lockable case or password protected portable device. Staff undertake to ensure these are kept out of sight and locked away when unattended.
- In the case of online provision, any videos of students submitted to the Service for reasons associated with teaching and learning or entering an online Jersey Eisteddfod festival, will be transferred using Government of Jersey approved email encryption and/or file sharing software.
- Any videos of students will be transferred to Government of Jersey approved secure storage and destroyed as soon as possible after use.
- Videos recorded by Jèrriais teaching staff will be recorded on password protected Government of Jersey recording equipment and transferred as soon as possible to Government of Jersey approved secure storage.
- Online teaching and Jersey Eisteddfod competition will take place using Government of Jersey approved online conferencing software. Participants will only be allowed entry on invitation.
- The use of Google Forms for collecting Jersey Eisteddfod competition Junior and Adult entries has been sanctioned by the Jersey Office for the Information Commissioner.

On the odd occasion, personal data is processed overseas using web services that are hosted outside the European Economic Area (EEA), for example Facebook. This is processed in the US, but has been approved by another competent supervisory authority under Article 40 of the GDPR or equivalent statutory provisions, together with binding and enforceable commitments of the controller and processor to apply the appropriate safeguards such as information security procedures and checks.

Policy author(s): Marianne Sargent
Date: November 2022
To be reviewed and updated: January 2024

Gouvèrnément d'JÈRRI