Department of Education

Data Protection Policy

1. Introduction – what is the policy for?

The Department of Education is mindful of its responsibilities with regard to the management of the requirements of the Data Protection (Jersey) Law 2018.

The Law is designed to protect the privacy of all individuals, known as data subjects under the law and will bring equivalence with the obligations brought to bear by the European GDPR (General Data Protection Regulation).

Schools and the Department and its various bodies will be acting as data controller(s) (and sometimes as data processor) for a wide variety of data processing activities, involving both personal and special category data.

SoJ (States of Jersey) Schools will be processing large volumes of children's data. All Schools and the SoJ have a responsibility to keep this data safe by keeping it secure and only processing it or sharing it when allowed by Law. It is illegal to process personal data without this legal safeguard. Failure to do so could not only compromise the trust that the public have in Schools and the Department, but could also result in enforcement action by the Information Commissioner.

This policy document sets out a framework through which effective management of data protection responsibilities and obligations can be achieved for the States of Jersey. This policy supersedes any previous States of Jersey Data Protection Policy.

The purpose of this policy is to ensure that the States of Jersey, and the employees and partners of the States of Jersey, comply with the provisions of the Data Protection (Jersey) Law 2018 when processing personal data.

This policy applies to:

- All SoJ employees (inclusive of all those that work in State Schools), and including on a voluntary basis and governors;
- Any individuals or third party organisations who are responsible for personal data on behalf of the States of Jersey as a public authority.

SoJ expects all Schools and individuals to be responsible and for staff to take seriously their role in handling personal data, however minor or transient a part it plays in their role. This policy applies regardless of where the data is held, for example if it is held or stored on personally-owned equipment or outside a School's or SoJ property, or if it is being processed on behalf of the SoJ or a School by a third party, such as a shredding service, consultant, or uploaded to a web based data hosting service.

1.1 Background to the GDPR and Data Protection (Jersey) Law 2018

The General Data Protection Regulation (GDPR), enforced May 25 2018, is European data protection legislation to replace the current 20-year-old EU data protection laws. It builds on current data protection legislation and is designed to harmonise data privacy laws across Europe. On the same

date, the Jersey Data Protection Laws are intended to produce equivalence to the principles of the GDPR.

1.2 The new data protection laws will strengthen current legislation by:

- At the first time we collect personal data we have to give them very clear and concise information on what we are going to do with their data, who they are going to share it with, what is the legal basis for processing it and how long we are going to keep it. This delivered through a privacy notice.

- Broadening what is considered personal data. For example, computer IP addresses could be considered personal data in some contexts.

- Making it mandatory to report a personal data breach (such as accidentally sending someone's personal information to the wrong person) to the Information Commissioner within 72 hours.

- Introducing fines of up to £10m for personal data breaches. (The States of Jersey will not be fined but sanctions will apply.)

- Strengthening citizens' rights to access information and to have it erased or corrected. It also enforces the right to data portability, giving people more ownership of their data so that they can move their information between service providers.

- Strengthening requirements around consent, so that people must opt in to receive information, such as direct marketing.

- Making it free for people to request information about themselves (Subject Access Requests or SARs), which previously incurred a fee. We will have to supply the requested information within 4 weeks.

- Providing enhanced protection for children's data.

- Removing the lawful basis of 'legitimate purpose' for public sector organizations such as SOJ.

- For the first time requiring Data Controllers to "demonstrate compliance" to the law and keep records of that compliance.

2. Terminology

The term '**School'** is used to describe Schools, Education Services and Youth Centres

What is 'personal data' **Personal data** means any data which relates to or identifies a living person. This definition is broad so be cautious that data that does not appear to be personal on the face of it, may well be. For example, the initials and job title of an employee, or a photo without a name on it are both personal data if you can identify the person from it. All personal data is covered by the Law, this includes both electronic data and data held on paper.

Personal data is context driven so remember before collecting new personal data an assessment will need to be made on the purpose, the necessity and the lawful basis on which you do so.

What is 'special category data' **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.

2.1 Special category data includes: (previously referred to as sensitive data)

- 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. 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, organization, 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. Anything you do with data is likely to fall within this definition.

Before processing any personal or special category data, all members of staff should consider the checklist below:

- Do you really need to record the information?
- Is the information 'personal' or is it 'special category'?
- If it is special category and is being transferred to a third party, do you have the appropriate data sharing agreement in place?
- Has the Data Subject been told that this type of data will be processed?
- Are you authorised to collect / store / process the data?
- If yes, have you checked with the Data Subject that the data is accurate?
- Are you sure that the data is secure?
- How long will you need to keep

Principles of data protection Staff are required to adhere to the principles of data protection as laid down by the Law. 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. Your responsibilities as a data controller

A data controller is the individual or organisation holding data and determines what happens to that data. Schools and other Education Department data controllers are responsible for a large amount of personal data, some of which is very sensitive.

All organisations will be required to keep a record of their processing, this called the data register detailing the why, where, how, when and what behind the processing of personal data. This an obligation to prove compliance with the law and record keeping.

It is expected as a public authority of the SoJ that schools follow guidance and advice and policy, and promote good practice set out by the Corporate Data Protection Team and Education Department.

This includes complying appropriately with subject access requests, reporting breaches and near misses correctly and investigating any complaints regarding data protection including requests to cease processing personal data.

If you no longer have a lawful basis process personal data the Data Guardian lead will review the retention dates of all the personal data processed by the organisation by reference to the data register, and they will identify any data that is no longer required in the context of the listed purpose. This data will be securely deleted/ destroyed in line with the Secure Disposal requirements detailed within the organisations retention policy.

3.1 All schools, by Law, must have a Data Protection Officer (DPO).

In order to provide assurance to Data Subjects and support to Data Controllers the law has introduced the role of a Data Protection Officer. The role is independent, not part of the data processing management team, who provides expertise in assuring your actions are within the law and in the best interests of the data subject.

The Data Protection Officer Responsibilities, Article 24 of the Law requires public authorities to appoint a Data Protection Officer. This can be an employee who is an expert in data protection and has no conflict of interest or can be procured under a service contract.

Part 5 of the Law sets out their statutory duties and responsibilities of the DPO. In order for a DPO to perform their role, the Law provides that they must be involved, properly and in a timely manner, in all issues that relate to the protection of personal data.

3.2 A DPO's duties include:

- informing and advising the organization of their obligations under the Law;
- monitoring 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;

- providing advice where requested as regards data protection impact assessments (DPIA) and monitoring the process covered by it; and
- having due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

3.3 It is **suggested** that ALL schools have a **designated compliance officer** to assist the DPO within a school. Some roles and responsibilities are more formalised than others. Each designated person is responsible for:

- liaising with, and cascading guidance provided by the Data Protection Team and The Department of Education;
- escalating data processing related issues to the Data Protection Officer, or Head of Governance at the Department of Education; and
- keeping their line manager informed of the above SoJ school and staff responsibilities. Staff members who process personal data about individuals in any capacity (however minor or fleeting) must comply with the requirements of this policy. Everyone has individual responsibility.

3.4 All staff members must ensure that:

- personal data is processed only in accordance with the Data Protection (Jersey) Law 2018
- all personal data is kept securely;
- Only those with a need to know should be given access to personal data;
- **work related emails should not be forwarded to personal email addresses;**
- no personal data is disclosed either verbally or in writing, to any unauthorised third party;
- personal data is kept in accordance with the SOJ retention schedule;
- any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Protection Team and/or the Corporate Data Protection Officer;
- any data protection breaches are swiftly brought to the attention of the Data Protection Team and that they support that Team as instructed in resolving breaches;
- ensure the Data Protection Officer is involved, and all queries and requests are examined properly and in a timely manner in all issues that relate to the protection of personal data, especially when members of staff are responsible for supervising or inducting children and non-permanent staff (such as voluntary or agency staff or work experience students) doing work which involves the processing of personal information, they must ensure that those students are aware of the data protection principles.

3.5 Processing of personal data by third parties

Schools and the SoJ still has legal responsibility for data when third parties are processing it. No School, 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 carried out. To be clear, the clicking 'yes' to terms and conditions on a web based service, or raising a purchase order, are all forms of contract.

If there is any doubt, you must get advice from your DPO or Head of Governance at the Department of Education.

Contractors, short-term and voluntary staff that are responsible for the use made of personal data by anyone working on its behalf. Managers who employ contractors, short term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing. In addition Senior Managers and/or designated person should ensure that:

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

4. Subject Access Request

The Data Protection (Jersey) Law 2018 provides individuals with a right to access to personal data which is processed about them by a data controller, such as a School. 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 the School and/or SoJ (or on the School's or SOJ'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 or their child if they have Parental Responsibility by the School and/or SOJ and this must be (with some exceptions) provided within four weeks. This right of access includes both electronic records and paper records. Schools must aim 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 SAR Point of Contact in the department.
- 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 and the Law Officers' Department. Schools and the SoJ are 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 be directed to the online portal at **https://www.gov.je/government/dataprotection/pages/subjectaccessrequest.aspx** where they will be directed to an online form.

Children, aged 13 and over, have the right to request how their personal data is being processed. If a parent requests a SAR for their child; the child will need to give their permission if aged 13 and over.

5. Privacy Notice

In order to ensure that processing of personal information is considered to be fair and lawful (Principle 1), it is essential that schools, in its role as data controller, ensures that the data subject has been provided with a 'Privacy Notice.' It must be uploaded to your website. It is important that the personal information processed is clearly and transparently identified, whom it is shared with and for what basis. It is illegal not to present a basis for which personal data is processed. The collection of information for one purpose cannot then be used for another purpose without explicit consent. Changes to the privacy statement must be made (and where appropriate to data sharing agreements).

The bases are as follows:

- Consent - offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation
- Contract - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- 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
- Vital Interests - processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Public Task - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Legitimate Interest - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (**N.B If you are a public authority, you cannot rely on legitimate interests for any processing you do to perform your tasks as a public authority and therefore this should NOT be a basis used to collect and process information in schools).**

It is important to review your privacy statement on an annual basis (or more regularly, if you implement new processes such as a cloud based service, CCTV etc.)

A generic template has been issued to your school for you to amend and include specific and relevant information pertaining to your school's particular activities.

6. Data Breach

The Data Protection (Jersey) Law 2018 defines a data breach like this:

"..personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed; Where a data protection breach occurs, or is suspected, it should be reported immediately in accordance with the data protection breach reporting process; via email to breach@gov.je or internally via the new incident reporting online form.

7. Parental Responsibility

Parental Responsibility describes the overarching rights and responsibilities for a child under the Children Law 2002. You don't have to have PR to make everyday decisions but does give rights over important issues such as which school a child attends, medical treatment, and who has sight of personal information about a child.

It is important to establish who has parental responsibility (PR) for each child at the outset, as only those with PR will have the right to access personal information regarding that child. Therefore, establishing PR early on will avoid difficulties later. PR can usually be established by looking at the birth certificate. (N.B. Jersey Law in this area is currently different from most other countries!)

How do we know who has parental responsibility?

A mother always has PR (unless it has been removed by a court). In the UK, Europe and most other countries, a father has PR if he is named on the birth certificate. **If the child was born in Jersey however, a father only has PR if he is named on the birth certificate AND was married to the mother at the time of birth** OR has subsequently married her OR has had PR subsequently given to him by a court. Sometimes a third party (such as a grandparent) may have been given PR by the court.

If PR has been conferred by a court order, you should ask to see the paperwork.

Schools should not accept what one parent says about PR without documentary evidence. If a parent registers a child for school and does not disclose details of the other parent, the school should ask for the birth certificate to confirm. If a parent states that the other parent is deceased or not contactable, they should put this in writing to the school.

<u>What if parental responsibility is in dispute?</u>

If a case is going through court, then the position is as it was prior to going through court. If a school is unsure as to who can collect a child or have contact while a case is going on, ask for a copy of the legal documents from the parents.

8. Privacy by Design

As part of the need to demonstrate compliance and ensure that we build in safeguards to all our new processes that collect personal data a key part of the Law is 'privacy by design.' This means that privacy/data protection is built into any project or data processing activity from the outset, rather than being added on retrospectively.

If you are planning to alter the way you collect existing personal data, introduce new computer systems or change suppliers that store your data you may to demonstrate a risk assessment before you implement this. Your DPO should be involved in any proposed changes at the outset to advise you on the right course of action.

Where a type of data processing is likely to result in a high risk to people's rights and freedoms, it is a legal requirement to carry out a data protection impact assessment, which is a way of implementing privacy by design.

More detailed guidance is available about what 'high risk' means, but in general terms, processing is high risk when:

- New technologies are involved;
- The processing is automated;
- It involves the processing of special category data on a large scale; or
- A systematic monitoring of a publicly accessible area on a large scale (e.g. CCTV
- When carrying out a data protection impact assessment, the data controller must seek the advice of the Data Protection Officer.
- A data protection impact assessment must contain the following minimum requirements:
- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- An assessment of the risks to the rights and freedoms of the individuals affected, and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Law, taking into account the rights and legitimate interests of any person.

The sponsor or owner of the project or data processing activity is responsible for ensuring the risk assessment is completed by the appropriate officers, who would be those with the most knowledge of the project.

9. Mitigations

Mitigations of any risk identified and should be regularly re-visited and amended as appropriate.

No high risk data processing should commence (even in pilot or beta phase) without the above being complete.

10. Overseas Transfers of personal data

Personal data should not be transferred to countries outside the European Economic Area (EEA) or 'adequate jurisdiction' without any other protection in place.

- Note that most web based applications (SIMS? Google, Apple, Yahoo, Facebook, Twitter etc.) may in fact transfer data outside of the EEA. Check the terms and conditions first. Many countries (including the U.S.) do not have data protection legislation. By sending a child's personal data to these jurisdictions, the safeguarding risks are increased.

- The default schools data protection registration with the Information Commissioner does not allow them to transfer data outside of the EEA. If you are transferring data to web based apps or other third parties hosted outside of the EEA, you must ensure appropriate security measures are in place and also update your registration with the Information Commissioner to 'worldwide' in order to be transparent and fair (Principle 1). In addition, to be 'fair' you must inform parents in your Privacy Notice, that you are transferring data worldwide and why.

- Appropriate safeguards may include (but not exhaustively):

    i) A contractual code of conduct together with binding and enforceable commitments of the receiver outside the EU;
    ii) Contractual clauses authorised by a supervisory authority;
    iii) Standard data protection clauses adopted by a supervisory authority and approved by the Commission;
    iv) An exemption; (such as a contract, in which you cannot perform the core purpose of the transfer without such a transfer. The use of Google Classroom is likely to fall under such an exemption).

11. **CCTV** (closed circuit television cameras) and audio recordings

It is important to remember that footage from CCTV cameras voice recordings also constitute personal data and will be covered by the Law and that the processing of that data must be fair and lawful, and adhere to all other principles of data protection.

For example someone making a subject access request could also ask for footage of themselves, and clear signage / privacy notices must be in place to tell people when they are being filmed /recorded and why. Please contact the Department at Edcompliance.gov.je if you have any queries, or the Central Data Protection Team at dataprotection2018@gov.je.

12. Register as a Data Controller

As a data controller, it is a legal requirement for you to register (notify) with the Information Commissioner. Your registration should be renewed annually and must accurately reflect the way in which you are processing your data. For example, if you are using CCTV or sharing data outside of Europe (for example via web based applications such as Google or Apple), this must be detailed in your registration.

You can check your registration status or renew your registration online at:

www.dataci.je