Data Protection

Policy, Procedures and Guidance

Data Protection Policy, Procedures and Guidance

Our Responsibilities as a Data Controller

The Data Protection (Jersey) Law 2005 is designed to protect the privacy of individuals and is almost identical to the UK Data Protection Act 1998.

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.

Under the Law, schools (and other Education Services such as the Youth Service and the Library) have a significant responsibility to keep this data safe by keeping it secure and only processing it or sharing it when appropriate. Failure to do so could not only compromise the safeguarding of young people, but could also result in prosecution.

Each school or educational establishment must have a member of its Senior Management Team as a point of contact for data protection. This individual would also be the point of contact for e-safety, records management and Freedom of Information.

Registration

As a data controller, it is our legal requirement to notify the Information Commissioner. Our registration is renewed annually and must accurately reflect the way in which we are processing your data.

- You can check our registration status at: www.dataci.je

What is 'personal data'?

- Personal data is data that relates to any living person that can be identified from that data (N.B. they do not have to be named - just identifiable. For example initials and year group would probably constitute personal data, as does a photograph, even if there is no name attached to it.)
- Examples of personal data would be: names, addresses, dates of birth, social security number, photographs, reports and payslips. The Law covers data held electronically as well as data held in hard copy.

What is 'sensitive personal data'?

Sensitive data is still personal data but of a higher level. Sensitive data is defined as anything involving physical or mental health, racial or ethnic origin, political opinions, religious beliefs, trade union membership, sexual life or criminal offences. Examples of sensitive data would be SEN details, a record of need, an accident report, or a parent's criminal record. There are certain conditions that have to be met before personal or sensitive personal data can be processed. These conditions are normally written consent, investigation of a crime or vital interests.

What is 'data processing'?

The following pages will discuss when we can and cannot 'process' personal or sensitive personal data. So it is important to define what processing means. Essentially, processing is an extremely broad term which encompasses photocopying, transferring, emailing, filing, destroying, putting in the post, sharing with police or another States Department etc. The following pages will explain when it is and is not appropriate to process data.

The information is taken from the Education Depts Data Protection Policy for Schools which acts as an umbrella policy for St. John's School.

The Data Protection Principles

Principle 1 - Fairly and lawfully

In order to be 'fair' a data controller must register with the Information Commissioner to declare what they are doing with data. Tell parents what you're doing with their child's data, the reasons for it, and don't do anything differently to what you've said you'll do. This is achieved via a 'fair processing statement' which go out in school induction packs.

In order to be 'lawful', personal data can only be processed if:

- The individual has consented
- Necessary for the performance of a contract (e.g. HR administration)
- Required under a legal obligation or required by statute or court order
- Necessary in order to pursue the legitimate interests of the data controller (e.g. education)
- Someone acting on the data subject's behalf who has their written consent
- Prevention or detection of crime
- National Security purposes
- For obtaining legal advice
- Preventing damage to health

In order to be 'lawful', SENSITIVE personal data can only be processed with:

- Explicit informed consent (i.e. a signed letter from a parent)
- Employment obligations (e.g. HR employee administration)
  Vital interests of data subject or another person. (e.g. medical emergency, child protection issues.)
- Non-profit organisations e.g. political, philosophical, religious, trade unions
- Information already been made public by data subject – deliberately (e.g. posting on Facebook)
- Legal proceedings/advice
- Public functions (e.g. income tax or social security issues)
- Medical purposes – health professional – preventative medicine
- Equal opportunity research

Principle 2 – Specified purpose

Personal data shall be obtained only for one or more specified and lawful purposes and not used for another purpose.

- For example, information collected for educational purposes cannot be used for marketing or distributing promotional leaflets produced for profit. You could not for example pass parental contact details to a recruitment agency to mailshot, as those details were given to you for educational purposes.

Principle 3 – Adequate, relevant, not excessive

- This is about record keeping. Do you actually require all the information you are holding – is it relevant? Are you holding too much? Are you holding enough?

- Ensure you are applying the retention schedules and not keeping data too long? It is important to use retention schedules rather than ad hoc judgements when destroying data. Contact the Head of Governance for your latest retention schedule.

Principle 4 – Accurate

- Is your data accurate and up to date? Do you regularly remind parents to keep you updated about their current address and phone number?
- Be proactive. When sending forms or data sheets to parents, include a statement requiring them to inform you of any change to the information provided.

Principle 5 – Not kept longer than necessary (for that purpose)

- Do you apply the retention schedules?
- Do you regularly weed personal information?
  If there is a good reason to keep it the information- for example if there has been an allegation (even if it is old) then you may decide to keep it for *another purpose* even if you would otherwise have destroyed the file in line with retention schedules. This is in order in certain circumstances, but the decision should be made and logged by the Headteacher.

Principle 6 – Data Subject Rights

A 'data subject' is the person to whom data relates. We are all data subjects and this principle sets out our rights in this regard. Data subjects have the right to ask any data controller for a copy of all personal data held about them. The individual can then object on the basis of direct marketing, damage and distress or inaccuracy. Any parent (or student) can also make such a request to a school. Not only would they be entitled to a copy of their file (or their child's file) but also any data (such as emails or meeting notes) that relate to them. However, exemptions may apply to some of the documents, which may need redacting. See section on 'Subject Access Requests' on how to deal with these requests.

Principle 7 – Security

- Data controllers must take adequate measures to safeguard personal data. This includes staff awareness training, locking computers when not in use and ensuring that visitors are unable to see the personal details of others on screen.
- A lost iPad, paper file, an email sent to the wrong place or hacked, or data uploaded to a website inappropriately, would all be breaches of the security principle.

Principle 8 – Overseas Transfer

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 (Google, Apple, Yahoo, Facebook, Twitter etc.) do 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 (see Principle 7) 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 fair processing statement that you are transferring data worldwide and why.

Transferring data to third party processors

School photographers, design agencies, shredding companies etc.

When using the services of a data processor (i.e. a third party who is processing data on your behalf), a written agreement (contract) must be in place. That contract must include suitable security arrangements. It is important to remember that if you use third parties in this way, you are only passing over the administration, **not** the responsibility. If that third party breaches the Data Protection Law, that breach will remain your responsibility as does the data, so it is imperative that no third party processor is used unless you have a written contract in place and have risk assessed the use of that service. Contact the Head of Governance for advice if you wish to draft a data sharing agreement.

Web based third party processors (e.g Google, Apple, Microsoft, Dropbox, Facebook, Twitter)

It is easy to overlook the fact that when you pass personal data to an educational application, or upload it via the internet to Google or any other web based service, you are effectively sharing that data with a third party data processor. This also applies to web mail and cloud based services.

Therefore all the guidelines above apply. You may not be able to obtain a bespoke written contract with a large company such as Google, however all such data sharing must be risk assessed (and this risk assessment documented) and the terms and conditions thoroughly considered before using such services. Bear in mind where the data is hosted (Principle 8) and ensure that you inform parents about this data sharing in your fair processing statement with parents (Principle 1).

You should not upload **sensitive** personal data to a web based service unless there are exceptional circumstances and you have written parental consent to do so (see Principle 1).

Electronic devices

The Security Principle of the Law must be adhered to at all times and in all contexts, regardless of location. Regardless of which device or server the data is held on and your geographic location, the data remains the responsibility of the school.

USB devices, iPads, laptops and so on must be password protected and kept secure.

Computers and devices should not be left unattended with personal data accessible and staff should not use unencrypted USB sticks or devices to store or transfer personal data.

Remote access

Particular care should be taken with remote access. The risks are inevitably higher. If you are logging on from a machine or device which is not yours, ensure that you log out before walking away from the machine and that nobody else can gain access or view your screen. Remember that the data is still the responsibility of the data controller, regardless of location or the device you are using.

E-mail

Email is not a particularly secure method of transferring information. It is easily hacked, forwarded or viewed by unauthorised individuals. You should not forward school emails to Hotmail, Gmail or any other web based email service.

If emailing sensitive information (and avoid this wherever possible), attach as a password protected Word document and call the recipient with the password. Password protecting a document only takes a few seconds and will go a long way to increasing your levels of security.

Do not include the password in the email, or any identifiable information on the header of the email.

Data Security around the building

Personal data should not be displayed on the walls where the public can see it. Many schools are used at the evenings and weekend for community use.

If there is personal information on noticeboards, consider covering it up at these times.

If sensitive information (e.g. medical information) is displayed in the staffroom, obtain the parent's consent to do so.

Make sure that computers do not print out to printers in shared areas where sensitive documents could be seen and ensure screens cannot be viewed through windows.

Parental responsibility (PR)

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!)**

<u>How do we know who has parental responsibility?</u>

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 is 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.

What about residence orders and maintenance?

A parent may say that the other child never stays with or sees the other parent or that he/she does not pay maintenance. These issues are not relevant to parental responsibility.

What if parental responsibility is in dispute?

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. If you are unsure as to how to progress, phone the Head of Governance on 449199.

Subject Access Requests

(Someone requests their own data or their child's data)
Under Principle 6 of the Law, individuals have the right to have access to their personal data i.e. data held about them (or their child, if they have parental responsibility). This is the most important of the data subject rights. This is called a Subject Access Request. The request must be in writing (email counts). No particular form or format is required but it must provide sufficient information to verify their identity and to enable a search to be carried out. A school may charge a **discretionary** £10 fee for this (or £30 in the case of an educational record).

Responses to subject access requests have to be made within 40 days of the receipt of the request. The clock does not start ticking until you have full information regarding the request and the requester. Information supplied will include all data (electronic or hard copy) that relates to the requester. This would include educational records, emails about or to the data subject, meeting notes or diary notes.

Do not supply the original files - keep copies. Exemptions may apply so you may need to redact the information before supplying. The most common exemption is third party information (for example if the file mentions other children). Seek advice from the Head of Governance for advice about more complex exemptions.

If a parent requests their child's data and the child is of the age of reason (the law is silent on age but guidance says around 12) then the child has a right over their own data and you may have to get their consent. Treat this on a case by case basis and seek advice.

Police Information Requests

Vital interest/ emergency situations**:** If it is a 'vital interest' situation e.g. missing or vulnerable child, or there is a fire or other emergency situation, the Data Protection Law enables you to share information with other agencies such as the Police with no other condition being met and you should co-operate fully and promptly.

Safeguarding / MASH information: There are protocols in place which enable sharing of safeguarding information with other agencies such as the police, health and social services. Each information request should be considered on a case by case basis however if a professional in one agency has raised concerns about a child, then it may be appropriate to share information. This decision to share information should be made only by the Headteacher / service manager (or person authorised by the Headteacher / service manager to do so). Seek advice from the Department if in doubt.

Investigation of a crime: If the information is being requested in relation to a crime, you can release information to the police (or other enforcement agencies). An article 29 is a formal form for information from the States of Jersey Police and you should ask for this to be completed in order to formalise the request, unless the time taken to do this would prejudice investigations. Note that this provision allows you to release information but does not compel you to release it. Ask the Department for advice if in doubt.

Court Order/ Summons: A court order compels you to release information.

Information Requests from other States Departments

All States Departments are distinct data controllers, so the provisions of the Law apply when sharing data. Vital interests would allow you to share data, as would child protection or emergency situations. Information sharing protocols are also in place for MASH information (see above). However, data should not be shared in other circumstances without written parental consent.

Information Requests from Lawyers

Remember that a lawyer is a third party data controller and you should not pass data to them unless a provision of the Law is met. Be particularly cautious if the request is related to a custody dispute as the lawyer will be representing one party and not the other.

You do not have to disclose information to a lawyer. You should not produce reports or letters about a child for a third party over and above what you would normally produce unless you are mandated to do so by a court order.

If you receive an information request from a lawyer, or are asked to appear in court, please refer it to the Head of Governance tel: 449199