St. John's Primary School

Data Protection

Policy, Procedures and Guidance

"You should be protected from things that could harm you."

Article 36 United Nations Rights of the Child

Thinking
Learning
Caring

This policy is written referencing:
https://www.gov.je/SiteCollectionDocuments/Education/P%20Data%20Protection%20Policies%20and%20Procedures%2020180910%20AM.pdf

Staff should also reference the St John's Data Protection- Staff "Need to Know" Leaflet- **Appendix 3**

Introduction

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).

At St John's we are acting as data controller (and sometimes as data processor) for a wide variety of data processing activities, involving both personal and special category data.

We process large volumes of children's data therefore we 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 at St John's School 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.

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

We are expected to take seriously our role in handling personal data. 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 School property, or if it is being processed on behalf of the School by a third party, such as a shredding service, consultant, or uploaded to a web based data hosting service.

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

The General Data Protection Regulation (GDPR), enforced 25th May 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.

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 are 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. There is an obligation to prove compliance with the law and record keeping.

It is expected as a public authority of the Government of Jersey, St John's will follow guidance, 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.

Data Protection Officer

All schools, by Law, must have a Data Protection Officer (DPO). At St John's this person is the Headteacher- Mr Jamie Hazley.

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.

A DPO's duties include:

- Informing and advising of 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
- Having due regard to the risk associated with processing operations, considering the nature, scope, context and purposes of processing

It is suggested that ALL schools have a designated compliance officer to assist the DPO within a school. At St John's School this person is Mrs Helen Falle (School Secretary)

Each designated person is responsible for:

- Liaising with, and cascading guidance provided by CYPES
- Escalating data processing related issues to the Data Protection Officer or Head of Governance

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 Government of Jersey 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

Processing of personal data by third parties

St John's School has legal responsibility for data when third parties are processing it. We will not 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 Government of Jersey 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 Government of Jersey 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 Government of Jersey 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

What is 'personal data'?

- Personal data is a much broader term than many initially realise, so be careful not to be caught out. 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 special category 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. Do we need to mention CP docs here?

Subject Access Request- SAR

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 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 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). 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 Government of Jersey 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 Government of Jersey 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 where they will be directed to an online form: https://www.gov.je/government/dataprotection/pages/subjectaccessrequest.aspx

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.

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.' This has been uploaded to our 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

The privacy Statement is reviewed annually.

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 **Edcompliance.gov.je**

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 will be built into any project or data processing activity from the outset, rather than being added on retrospectively.

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 (DPIA), which is a way of implementing privacy by design.

What is 'data processing'?

Essentially, processing is an extremely broad term which encompasses photocopying, transferring, emailing, filing, destroying, putting in the post, sharing with police or another Government of Jersey Department

Fair, lawful and transparent processing

Personal data are to be processed lawfully, fairly and in a transparent manner in relation to the data.

To ensure lawful processing of personal data, the controller or processor must meet at least one of the conditions specified in Schedule 2- **Appendix 2**. No single basis is better or more important than the others – which basis is most appropriate to use will depend on the organisation's purpose and relationship with the individual.

At least one of these must apply wherever an organisation processes personal data:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task

- Legitimate interests

An organisation must determine the lawful basis before processing begins and it should be documented. The basis for processing should be documented in any privacy notice.

To ensure your processing is fair and transparent, controllers and processors must consider how the data are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purposes for which they are to be processed.

In order that personal data may be processed fairly and transparently, a controller must –

- Facilitate the exercise of the rights of data subjects
- Act on a data subject's request unless the data

Purpose Limitation

Personal data must be collected for specified, explicit and legitimate purposes and once collected, not further processed in a manner incompatible with those purposes.

This means controllers and processors cannot obtain personal data for one purpose and then go on to use it for another incompatible purpose. Every new purpose must have its own legal basis and the purpose must be defined before processing is started.

Excessive Data Collection

Personal data collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

This Principle is to ensure compliance with the concept of data minimisation, meaning that controllers and processors should only collect personal data that is sufficient for the purposes for which it is required. You should identify the minimum amount of personal data you need to properly fulfil your purpose. You should hold that much information but no more than that and you should not keep information simply on the basis that it might be useful in the future but where you have not actual need for it.

Accuracy of Data

Personal data must be accurate and, where necessary, kept up to date, with reasonable steps being taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

This Principle requires controllers and processors to take steps to ensure the continued accuracy of the personal data they hold. This might be through routine interactions with customers, certain trigger events or an annual review of customer databases. If the information is used for a purpose that relies on it remaining current, it should be kept up to date i.e., employee payroll records should be updated when an employee receives a pay rise.

Storage Limitation

Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.

This Principle relates to the retention of personal data and requires that controllers and processors do not retain personal data for longer than is necessary for the purposes for which it was obtained. The Law does not set out any specific minimum or maximum periods for retaining personal data; it is for the organisation to assess how long they need to keep the data for, and why. Ensuring personal data is disposed of when no longer needed will reduce the risk that it will become inaccurate, out of date or irrelevant.

Data Security, Integrity and Confidentiality

Personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

This Principle requires controllers and processors to ensure the appropriate technical and organisational measures are in place to protect the personal data they hold. This means the development of robust data security systems and confidentiality policies and procedures. It also means training staff to ensure they know how to keep personal information safe.

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.

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 (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 school's 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; 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).

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

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

Change History

Version	Date Issued	Issued by	Reason for Change	Presented To	Approved by:	Date
0.1	November 2019	Trudie De La Haye				
0.2	November 2022	Jamie Hazley	Updated to include General Data Protection Regulation (GDPR) from May 2018	SLT	Jamie Hazley	

Appendix 1- St John's Privacy Notice

St. John's Primary School Jersey
Privacy Notice 2022

St. John's 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 States 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.

WHAT

What information do we collect about you?

We collect the following types of information about you:

- 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
- Contact Tracing and Positive Cases

WHY

Why do we collect information about you?

We need to collect and hold information about you, 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
- 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
- Allow the statistical analysis of data so we can plan the provision of services
- Comply with the law regarding data sharing
- Where necessary to protect individuals from harm or injury, including anything that could harm health.

HOW

How will we use the 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. A retention schedules are in place which determines 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 States 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 do, on the odd occasion, process your information overseas using web services that are hosted outside the European Economic Area, for example Facebook and Twitter. 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.

We upload children's data to the MiS (SIMS Database) that is hosted in the European Union. In addition, children's data in Early Years Foundation Stage (EYFS) is also uploaded to EExAT. All of these services are hosted within the European Union. To understand how this information is processed in more detail please read Appendix A.

Data Sharing

We may need to pass your information to other States of Jersey (GOVERNMENT OF JERSEY) departments or organisation to fulfil your request for a service. These departments are Health, Social Services, Social Security, Multi trust agencies. 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, etc.

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.

Publication of your information	E-Mails	Telephone Calls
We may need to publish your information on our website and/or in the Jersey media for the following reasons: • Where we are required by law to publicise certain information, for example performance data. • In the interests of demonstrating a fair and transparent decision-making process, for example admissions process and appeals procedure. • Where we are required to provide statistical information about a group of people; although your data will be anonymised to protect your identify. • Where you have responded to a public consultation, although your comments will be anonymised to protect your identity.	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	We do not record or monitor any telephone calls you make to us using recording equipment. 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.

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.	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.

Email: admin@stjohn.sch.je

You 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. However where our records are not held in a way that easily identifies you, for example a land registry, 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

You can complain to us about the way your information is being used

If you have an enquiry or concern regarding the processing of your personal data please contact:

Telephone: +44 (0)1534 861692

Email: admin@stjohn.sch.je

St. John's Primary School
La Rue de la Mare Ballam,
St. John
JE3 4EJ

You can also complain to the Information Commissioner about the way your information is being used

The Office of the Information Commissioner can be contacted in the following ways:

Telephone: +44 (0)1534 716530

Email: enquiries@jerseyoic.org

Office of the Information Commissioner
2nd Floor,
5 Castle Street,
St Helier, Jersey, JE2 3BT

Appendix 2- The Data Principles – Office of the Information Commissioner

SCHEDULE 2: CONDITIONS FOR PROCESSING OF PERSONAL DATA PART 1 – CONDITIONS FOR PROCESSING PERSONAL DATA

1 Consent

The data subject has consented to the processing of his or her data for one or more specific purposes.

2 Contract

The processing is necessary for –

(a) the performance of a contract to which the data subject is a party; or

(b) the taking of steps at the request of the data subject with a view to entering into a contract.

3 Vital interests

The processing is necessary to protect the vital interests of the data subject or any other natural person.

4 Public functions

The processing is necessary for –

(a) the administration of justice;

(b) the exercise of any functions conferred on any person by or under any enactment;

(c) the exercise of any functions of the Crown, the States or any public authority; or

(d) the exercise of any other functions of a public nature with a legal basis in Jersey law to which the controller is subject and exercised in the public interest by any person.

5 Legitimate interests

(1) The processing is necessary for the purposes of legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, unless –

(a) the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject, in particular where the subject is a child; or

(b) the controller is a public authority.

(2) The States may by Regulations specify particular circumstances in which the condition set out in sub-paragraph (1)(a) is, or is not, to be taken to be satisfied.

PART 2 – CONDITIONS FOR PROCESSING PERSONAL DATA AND SPECIAL CATEGORY DATA

6 Consent

The data subject has given explicit consent to the processing for one or more specific purposes.

7 Other legal obligations

The processing is necessary for compliance with a legal obligation, other than one imposed by contract, to which the controller is subject.

8 Employment and social fields

The processing is necessary for the purposes of exercising or performing any right, obligation or public function conferred or imposed by law on the controller in connection with employment, social security, social services or social care.

9 Vital interests

The processing is necessary in order to protect the vital interests of –

(a) the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the controller cannot reasonably be expected to obtain the consent of the data subject; or

(b) another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

10 Non-profit associations

The processing –

(a) is carried out in the course of its legitimate activities by any body, or association, that is not established or conducted for profit, and exists for political, philosophical, religious or trade union purposes;

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects;

(c) relates only to individuals who are members of the body or association or have regular contact with it in connection with its purposes; and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

11 Information made public

The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

12 Legal proceedings

The processing is necessary for the purposes of –

(a) any legal proceedings;

(b) obtaining legal advice; or

(c) establishing, exercising or defending legal rights.

13 Public functions

The processing is necessary for –

(a) the administration of justice;

(b) the exercise of any functions conferred on any person by or under an enactment; or

(c) the exercise of any functions of the Crown, the States, any administration of the States or any public authority.

14 Public interest

The processing is necessary for reasons of substantial public interest provided for by law and is subject to appropriate protections to protect the rights and interests of the data subject.

15 Medical purposes

(1) The processing is necessary for medical purposes and is undertaken by –

(a) a health professional; or

(b) a person who in the circumstances owes a duty of confidentiality equivalent to that which would arise if that person were a health professional.

(2) In paragraph (1) “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment, the management of healthcare services, occupational medicine and the assessment of the working capacity of the employee.

16 Public health

The processing is necessary for reasons of public interest in the area of public health, including (but not limited to) protecting against cross border threats to health and ensuring a high standard of quality and safety of health care or social care where they are provided for by law and the processing is carried out with appropriate safeguards for the rights and freedoms of data subjects.

17 Archiving and research

The processing:

(a) is in the public interest;

(b) is necessary for the purposes of archiving or for statistical, scientific or historical research;

(c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of the data subject; and

(d) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

18 Avoidance of discrimination

(1) The processing –

(a) consists of information as to –

(i) any protected characteristic within the meaning of the Discrimination (Jersey) Law 2013[35], or

(ii) a person’s disability, or

(iii) a person’s religious beliefs;

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment of persons on grounds of any characteristic described in clause (a)(i) to (iii) with a view to enabling such equality to be promoted or maintained;

(c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of the data subject; and

(d) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The processing is not contrary to any notice in writing that an individual has given to the controller requiring the controller to cease processing personal data in respect of which the individual is the data subject, such notice taking effect at the end of a period that is reasonable in the circumstances or, if longer, the period specified in the notice.

19 Prevention of unlawful acts

The processing –

(a) is in the substantial public interest;

(b) is necessary for the purposes of the prevention or detection of any unlawful act or unlawful omission; and

(c) in order not to prejudice those purposes, is required to be carried out without the controller’s seeking the explicit consent of the data subject.

20 Protection against malpractice and mismanagement

The processing –

(a) is in the substantial public interest;

(b) is necessary for the discharge of any function that is designed for protecting members of the public against –

(i) dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person, or

(ii) mismanagement in the administration of, or failures in services provided by, any body or association; and

(c) in order not to prejudice the discharge of that function, is required to be carried out without the controller's seeking the explicit consent of the data subject.

21 Publication about malpractice and mismanagement

(1) The processing –

(a) takes the form of disclosure;

(b) is in the substantial public interest;

(c) is in connection with –

(i) the commission by any person of any unlawful act, or unlawful omission, whether alleged or established,
(ii) dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person, whether alleged or established, or

(iii) mismanagement in the administration of, or failures in services provided by, any body or association, whether the mismanagement or failures are alleged or established;

(d) is for the special purposes; and

(e) is made with a view to the publication of those data by any person.

(2) The person who is the controller in relation to the processing reasonably believes that the publication would be in the public interest.

22 Counselling

(1) The processing –

(a) is in the substantial public interest; and

(b) is necessary for the discharge of any function designed for the provision of confidential counselling, confidential advice, confidential support or a similar confidential service.

(2) One or more of the following conditions is satisfied –

(a) the data subject cannot give consent to the processing;

(b) the controller cannot reasonably be expected to obtain the consent of the data subject to the processing; or

(c) the processing must, in order not to prejudice the discharge of the function referred to in sub-paragraph (1)(b), be carried out without the controller's seeking the explicit consent of the data subject.

23 Insurance and pensions: general determinations

(1) The processing –

(a) is necessary for the purpose of –

(i) carrying on insurance business falling within Class I, III or IV of Part 1 of Schedule 1 to the Insurance Business (Jersey) Law 1996[36], or within Class 1 or 2 of Part 2 of that Schedule, or

(ii) making determinations in connection with eligibility for, or benefits payable under, an occupational pension scheme, being a scheme, or arrangement, that is constituted in one or more instruments or agreements and has, or is capable of having, effect in relation to one or more descriptions or categories of employments so as to provide benefits, in the form of pensions or otherwise, payable on termination of service, or on death or retirement, to or in respect of earners with qualifying service in an employment of any such description or category; and

(b) does not support measures or decisions that relate in particular to the person who is the data subject in respect of the personal data.

(2) The controller cannot reasonably be expected to obtain the explicit consent of that data subject to the processing and the controller is not aware of the data subject's withholding his or her consent to the processing.

(3) The personal data consists of information relating to the physical or mental health or condition of a data subject who is the parent, grandparent, greatgrandparent or sibling of –

(a) in the case of processing for the purpose referred to in subparagraph (1)(a)(i), a person insured (or seeking to be insured) in the course of the insurance business; or

(b) in the case of processing for the purpose referred to in subparagraph (1)(a)(ii), a person who is a member of the scheme or seeking to become a member of the scheme.

24 Insurance and pensions: current processing

(1) The processing –

(a) was already under way in relation to the same data subject and by or on behalf of the same controller immediately before the coming into force of this Schedule; and

(b) is necessary for the purpose of –

(i) carrying on insurance business falling within Class I, III or IV of Part 1 of Schedule 1 to the Insurance Business (Jersey) Law 1996, or

(ii) establishing or administering an occupational pension scheme, being a scheme, or arrangement, that is constituted in one or more instruments or agreements and has, or is capable of having, effect in relation to one or more descriptions or categories of employments so as to provide benefits, in the form of pensions or otherwise, payable on termination of service, or on death or retirement, to or in respect of earners with qualifying service in an employment of any such description or category.

(2) One or both of the following conditions is satisfied –

(a) the controller cannot reasonably be expected to obtain the explicit consent of the data subject to the processing and has not been informed by the data subject that the latter refuses consent to the processing;

(b) the processing must, in order not to prejudice the purpose referred to in sub-paragraph (1)(b), be carried out without the controller's seeking the explicit consent of the data subject.

25 Functions of a police officer

The processing is necessary for the exercise of any function conferred on a police officer by or under any enactment or other law.

26 Regulations

Regulations may –

(a) specify further circumstances in which special category data are processed;

(b) exclude the application of this Schedule in such cases as may be specified;

(c) provide that, in such cases as may be specified, any condition in this Schedule is not to be regarded as satisfied unless such further conditions as may be specified in the Regulations are also satisfied; or

(d) specify circumstances in which processing falling within paragraph 17(a) and (b) is, or is not, to be taken for the purposes of paragraph 17(d) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

Appendix 3- St John's Data Protection- Staff "Need to Know" Leaflet

Gathering and Processing Data
Personal data must be collected for specified, explicit and legitimate purposes and once collected can only be used for the identified purpose. This means we cannot obtain personal data for one purpose and then go on to use it for another incompatible purpose.
Data processing is an extremely broad term which encompasses photocopying, transferring, emailing, filing, destroying, putting in the post or sharing data with any other agency.

DATA FOR NOW

It is IMPERATIVE all staff to speak with Mr Hazley or Mrs Falle prior to gathering data or processing children's data

St. John's Primary School

Data Protection

What do I need to know?

Thinking Learning Caring

The General Data Protection Regulations (GDPR) give individuals more choice and control over how their data is used however it does create an "air of confusion." This factsheet is designed to help you feel confident about how we all can use and protect data at St John's.
The regulations bring in stricter duties, which all organisations, including schools, must follow.
Failure to comply with legislation could have far reaching implications, therefore compliance with our Data Protection Policy is essential.
All staff will have a responsibility to ensure that their own activities comply with GDPR.

Actions to observe at St John's are:

a. Keeping files locked away.
b. Use the confidential waste bin where data is no longer needed.
c. Adhere to the clear desk policy.
d. Lock your computer screen when you are away from your desk.
e. Encrypt removable media USBs (memory sticks), CDs etc so that if they are lost the data cannot be accessed.
f. Taking care if working in public- who may be able to see your screen
g. Dispose of personal information as soon as you no longer it for e.g., post school trips

What you need to know

1) GDPR covers all processing of personal data. This applies to any personal data that is processed about our pupils
2) Mr Hazley has the designated responsibility for data protection (Data Protection Officer) matters, including GDPR. He is responsible for ensuring that personal data is correctly collected, stored, used and securely destroyed once it is no longer needed.
3) We have robust procedures to deal with data protection breaches. A data breach is anything leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data. Most breaches are the result of human error. All breaches need to be reported to the Information Commissioner's Office
4) You should never disclose any personal data outside of your school's procedures, or use personal data held on others for your own purposes.
5) You should take extra care to ensure that any personal data that you use at school is kept secure.

When things do go wrong:
Where a data protection breach occurs, or is suspected, it should be reported immediately to the School Data Protection Officer (Mr Hazley) in accordance with School Policy. He in turn will report the breach via email to edcompliance.gov.je
Examples of breach that MUST be reported to the DPO- Mr Hazley:

i. Paper files or USB sticks are lost.
ii. An email containing personal data is sent to the wrong person in error. Sometimes the incorrect recipient will have the same name as the intended recipient.
iii. An email is sent to a group of people using the CC field rather than the BCC field, therefore disclosing everyone's email address to everyone else.
iv. Personal data is left on desks unsecured.
v. An incorrect document containing personal data is attached to an
vi. email in error.