Data Protection Policy

This Policy outlines how James Brindley employees must meet the requirements of the Data Protection Act 1998.

Any queries arising from this Policy or its implementation can be taken up directly with the Senior Information Risk Officer

Senior Information Risk Officer (SIRO) – John Bradshaw
Data Protection Registration reference number Z519817X

Table of Contents

1 Scope

This policy applies to all elected members, employees, or any other person with access to personal or sensitive information processed by James Brindley School.

The policy covers the obtaining of personal data, its storage and security, its use and its ultimate deletion or disposal

The policy should be read in conjunction with

- Freedom of Information Policy
- Acceptable Use of the Internet Policy
- Record Keeping Policy

2 Introduction

Everyone managing and handling personal information needs to understand their responsibilities in complying with the Data Protection Act 1998 (the Act).

This policy covers all personal data, however they are held, on paper or in electronic format, and the rights of individuals (data subjects) who wish to see information the School holds about them (by submitting a Subject Access Request).

It is a legal requirement that the School complies with the Act, and all members of staff have a statutory responsibility to ensure the School's legal compliance.

This policy is intended to facilitate compliance and all staff should be aware of its content and the key requirements of the Act. Managers should ensure that staff are provided with the appropriate knowledge and training to ensure they can fulfil their responsibilities.

3 Responsibilities

Whilst the School's Head Teacher is ultimately responsible, both personal and corporate responsibility applies. All employees are therefore responsible for ensuring compliance with the Principles of the Data Protection Act by complying with this policy.

Line managers must ensure that those staff managing and handling personal information are adequately trained and supervised with regard to the requirements of this policy.

Senior Information Risk Officer (SIRO) will monitor the School's compliance with the Act, ensure that the Data Protection Policy is implemented, advise and consult on responses to data Subject Access Requests and make annual reviews of this policy and associated documentation.

4 Definitions

Personal data is information which relates to a living individual who can be identified:

- From those data
- From those data when combined with other information which is either in the School's possession or likely to come into the School's possession.

For the purposes of the Act, and the School's Data Protection Policy, it is safest to assume that all information about a living, identifiable individual is personal data and should be dealt with accordingly.

Sensitive Personal Data can include information relating to

- Religious belief or other beliefs of similar nature
- Sexual life
- Physical or mental health conditions
- Member of a trade union
- Political opinions
- Commission or alleged commission of an offence
- Proceedings for any offence committed or alleged to have been committed
- Racial or ethnic origin

Sensitive data must only be used for approved purposes (e.g. equal opportunities monitoring) and access to this data must be restricted to those who have a need to know. They should never be kept in a generally accessible record or file. Advice on the issue of sensitive data can be sought from the Data Protection Officer.

5 The Principles of the Data Protection Act 1998

The eight principles which form the basis of the Act state that data must be:

1) Fairly and lawfully processed
Data must be processed fairly and lawfully. Nobody should be deceived or misled about the purpose for which their data is to be processed.

2) Processed for limited purposes
Personal data can only be obtained for specified and lawful purposes with permission from the data subject for each purpose.

3) Adequate, relevant and not excessive
The data must be sufficient to meet their purpose but not provide more information than the purpose requires, or provide information outside the scope of the purpose.

4) Accurate

The personal data must be accurate when recorded, and accuracy must be maintained throughout the lifecycle of the data.

5) Not kept for longer than is necessary.

Personal data must not be kept for any longer than is necessary for the purpose for which it was obtained. If data are kept for too long, the accuracy and relevance may be compromised.

6) Processed in line with the rights of the subject of the data

Data subjects have the right to access their personal data and can request the termination of any processing that causes or is likely to cause them distress. They can insist that their data is not used for marketing and other purposes, and can request that inaccurate data is amended.

7) Stored and processed securely

All necessary measures must be taken to prevent unauthorised or unlawful processing of personal data and to protect personal data against loss, damage or destruction.

8) Not transferred to countries without adequate protection

Personal data must not be transferred to a country outside the European Economic Area (i.e. the EU member states, Norway, Iceland and Liechtenstein) unless that country has in place a level of data protection comparable to that in the EU. Advice should be sought from the Data Protection Officer.

On entry to the school pupils and staff will be informed that data may be stored in the cloud. This will be held in the European Economic area where possible. In instances where it is held elsewhere, that country will have in place a level of data protection comparable to that in the EU

6 Processing Personal Data

The definition of processing in relation to data protection is very wide. Obtaining, holding, filing, organising, transmitting, retrieving, disseminating, disclosing and destroying of data are all deemed to be processing in addition to any other process that is carried out on the data.

Members, employees and others acting on behalf of the School must only have access to personal data that are necessary in order to carry out their duties and responsibilities.

All forms used to obtain personal data, such as application forms or registration forms must:

- State the purpose/s for which the information is required
- Be reviewed regularly to check that all of the information asked for is still required and necessary.
- Be checked for the accuracy of the data before they are used for any processing. If in doubt about the accuracy of the data they should be referred back to the data subject for confirmation

Personal data must be collected and handled in a way that complies with the Act and meets the eight principles above. This imposes a duty on the School to ensure that individuals are made aware of the uses that will be made of the information that they supply and give their consent to this.

If data are provided by an outside agency then the agency must be asked to confirm in writing that the data were obtained fairly and lawfully, in compliance with the Act.

Any information held regarding criminal convictions must be treated as sensitive information and handled accordingly. Any request made by the School for such information must be fully justified. Advice should be sought from the Data Protection Officer at Birmingham City Council.

7 The Purpose of the Data

In addition to obtaining consent, the data must be used only for the declared purpose/s, which the School has notified to the Information Commissioner's Office.

If there is a new purpose or change to an existing purpose then the School's Data Protection Officer must notify the Information Commissioner's Office immediately.

Processing of data cannot begin for the new or amended purpose until the Commissioner has accepted this notification.

The School's registration entry with the Information Commissioner's Office can be seen via the intranet or from the Senior Information Risk Officer (SIRO).

8 Relevant and Adequate Data

The School must process only that information which is necessary to fulfil the business requirement or which is needed to comply with legal requirements. For example it is not necessary to ask about a driving licence on a job application form if the post applied for does not entail any driving duties.

9 Collecting Accurate Data

Errors in personal data that cause data subjects damage or distress could lead to the School being prosecuted. It is important therefore that all appropriate measures are put in place to verify the accuracy of data when they are collected, especially when any significant decisions or processes depend upon the data.

There is a requirement to ensure that data are kept up to date throughout the lifecycle of the data.

10 Keeping Data ONLY AS LONG AS NECESSARY

Retention periods should be defined for personal data and procedures put in place to ensure compliance.

Retention periods must be for clear business purposes and must be documented to identify why certain records are retained for certain periods of time.

Refer to the Retention of Records Policy for further guidance

When no longer required, data must be deleted or disposed of securely. Further information on this is available from the SIRO.

11 Safeguarding the Rights of Data Subjects

Individuals have various rights under the Act. These are: -

- The right to be told that processing is being carried out
- The right of access to their personal data
- The right to prevent processing in certain cases
- The right to have inaccurate or incorrect information corrected, erased or blocked from processing.

12 Subject Access Requests

The School must make available details of how individuals can request access to their data, by means of a Subject Access Request.

Subject Access Requests must be made in writing and sufficient detail must be obtained to ensure that the request has been made by the data subject in person.

As proof of identity at least two identifying documents of the data subject, such as a driving licence, passport, recent utility bill etc. must accompany the request. If a third party is making the request, a signed letter of consent from the data subject should also be enclosed.

The request must then be passed to the SIRO within 24 hrs

Subject Access Requests must be satisfied within 40 calendar days of their receipt by the School.

It is not permitted to give personal data to third parties unless it is already in the public domain, or authorised by the data subject.

Informal requests to view or have copies or personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the 40 day time limit.

In certain circumstances, the courts, police or Inland Revenue may have the right of access to personal data without prior permission or knowledge of the individuals concerned. Any such request should be referred to the Data Protection Officer via the BCC Data Protection Centre.

This policy will be included in the Staff Handbook.

Data Protection statements will be included in the school prospectus and on any forms that are used to collect personal data.

13 Recognising and labelling sensitive data

All documents that contain protected data must be labelled as such with clear handling notes and practice is currently developing across the school in line with new guidelines.

Determining and Managing the Impact Levels

The school will label all sensitive data with Impact Levels 1 to 4 following the guidelines set out below:

Impact Level Description	Level 1	Level 2	Level 3	Level 4
Reason	General Document	likely to cause embarrassment to an individual or organisation	Likely to cause loss of reputation to an individual or organisation	Likely to cause embarrassment or loss of reputation to many citizens or organisations
Example	A general report or note which could be seen by anyone. No names or other personal details are listed in the document.	Basic information on an individual i.e. Name, DOB Class	Detailed information on an individual i.e. IEP etc. or basic information about a group - i.e. Class list with DOB	Detailed information about a group - i.e. Exam results with names and addresses of students. Child protection documents
Impact Level	**Level 1 - Not protectively Marked**	**Level 2 - Protect**	**Level 3 - Restricted**	**Level 4 - Confidential**
JBS Examples	• Policies • Worksheets • SOW • Lesson Plans	• Speech & Language. • Inter school e-mails / communication . • Context sheets	• OT information communication . • Advice/ Concerns re individual pupils. • Emailing E.P information. • QA of WAGs L drive. • RFD's. • Informing schools that	• Inter school e-mails / communication. • Confidential emails about staff performance. • Confidential emails about staff absence. • Referrals to other agencies e.g. YOT, Space, Stepping Stones. • Information relating to medical needs (emails to doctors)

			children are now dual registered with JBS and paper work associated. • Internal assessment WAG sheets L drive. • Taxi applications & Risk assessment. • Email L.S.P's Connexions. • Pupil support plans/ attendance plans. • Individual risk assessments. • IEP's • Pupil support plans • Videos of pupils rehabilitation	• Child Protection referrals • Individual risk assessments. • Individual pupil risk assessments. • Statements • Child Protection all documents. • Annual review information. • Administration of medication consent/ care plan. • Teacher appraisal, lesson observations. • Any information related to individual pupil where name /DoB • Consultants letters • Special consideration sent to Deb & have schools • Case Studies
Storage	• H drive • FROG • CLOUD • No Prefix	• L drive • School • Prefix D2	• L drive • Prefix D3	• L drive • Prefix D4
Communication	• Email	• Email	• Access via VPN at home • Internal emails • External emails must be password encrypted	• Access via VPN at home • Internal emails point to a location on the L drive • External emails password encrypted (password must be sent via a phone call) • Share file system

14 Keeping Data Secure

The School acts as custodian of personal data (data controller) and must therefore ensure that necessary and sufficient precautions are in place to prevent misuse or unauthorised access to data as well as having security measures in place to prevent loss or damage to data.

Filing cabinets containing personal data must be locked outside of normal working hours and keys must be held securely by nominated staff.

Electronic files must be password protected and passwords must be changed on a regular basis.

All such electronic data must be stored in secure server areas, not on computer hard drives, laptops or other mobile devices.

Backing up of electronic data will be held securely on an alternative site or when off-site it will be encrypted, password protected with access by named JBS staff only.

If any data are to be taken from the office (e.g. to work at home) then the data must be held securely at all times whilst in transit and at the location they are being held. In particular data must be protected from unauthorised access.

Data should not be held on staff personal devices.

Where outside bodies process or hold any of the School's personal data then the School must be satisfied that the data is held securely and with due regard to the obligations of the Act.

As part of the exit interview staff are required to confirm they have returned all school data.

15 Transfer of Data

As most complication occur when documents are transferred between systems and sites it is imperative that all staff conform to the 'Out of School Access' as defined in Section 13 Recognising and labelling sensitive data.

Data must not be transmitted or transferred out of the European Economic Area (i.e. the EU member states, Iceland, Norway and Liechtenstein) unless the country they are being transferred to has the same or equivalent standards of Data Protection. This has implications for data placed on the Internet and use of e-mail where servers are based abroad.

School equipment should not be taken outside the country to access/process data.

If information is required to be transferred abroad then checks must be made to ensure that the data are held securely during transfer and that data recipients apply data protection rules equivalent to those in the UK Data Protection Act 1998. Advice on this should be sought from the Data Protection Officer.

16 Breech action protocol

If there is a breach of school data whether it's a stolen/lost/misplaced iPad or even if a malicious hack is expected, staff must report it to the ICT department, and head of sector, as soon as they are aware.

We will remote wipe school equipment to prevent any data loss when the device next touches a network. Staff will also need to fill in the Data Loss Form, pass it to head of sectors who will examine it before returning it to the ICT technicians and responsible member of SLT, within two hours of the breach. A decision will then be made based on what is on the device as to the next steps regarding ICO