The Joseph Rowntree School
the right school to grow in

Information Policy

Reviewed by: School Business Manager (Veritau Adopted Policy)

Date of Adoption by Governing Body: FSR 15th June 2020

Chair of Governor's Signature: _____

Date to be Reviewed: June 2021

INTRODUCTION

This policy is to ensure that The Joseph Rowntree School complies with the requirements of the General Data Protection Regulation, The Data Protection Act 2018, Environmental Information Regulations 2004 (EIR) and Freedom of Information Act 2000 (FOIA), associated guidance and Codes of Practice issued under the legislation.

SCOPE

The Information Policy applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post / courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

This policy is the School's main information governance policy and addresses:

- Data Protection (including rights and complaints)
- Freedom of Information
- Information Asset Management

Information Security Incident Reporting is covered at Appendix 1.

DATA PROTECTION

Personal data will be processed in accordance with the requirements of GDPR and in compliance with the data protection principles specified in the legislation.

The school has notified the Information Commissioner's Office that it is a Data Controller and has appointed a Data Protection Officer (DPO). Details of the DPO can be found here:

Information Governance
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL
schoolsDPO@veritau.co.uk
01609 53 2526

The DPO is a statutory position and will operate in an advisory capacity. Duties will include:

- Acting as the point of contact for the Information Commissioner's Office (ICO) and data subjects;

- Facilitating a periodic review of the corporate information asset register and information governance policies;
- Assisting with the reporting and investigation of information security breaches
- Providing advice on all aspects of data protection as required, including information requests, information sharing and Data Protection Impact Assessments; and
- Reporting to governors on the above matters

INFORMATION ASSET REGISTER

The DPO will advise the school in developing and maintaining an Information Asset Register (IAR). The register will include the following information for each asset:

- An individual information asset identification number;
- The owner of that asset;
- Description and purpose of the asset;
- Whether there is a privacy notice published for that asset;
- Format and location of the asset;
- Which officers (job titles / teams) have routine access to the information;
- Whether there are any data sharing agreements relating to the information and the name of that agreement,
- Conditions of data processing;
- Details of any third parties contracted to process the information;
- Retention period for the asset

The IAR will be reviewed annually and the School Business Manager will inform the DPO of any significant changes to their information assets as soon as possible.

INFORMATION ASSET OWNERS

An Information Asset Owner (IAO) is the individual responsible for an information asset, understands the value of that information and the potential risks associated with it. The school will ensure that IAO's are appointed based on sufficient seniority and level of responsibility.

IAO's are responsible for the security and maintenance of their information assets. This includes ensuring that other members of staff are using the information safely and responsibly. The role also includes determining the retention period for the asset, and when destroyed, ensuring this is done so securely.

TRAINING

The school will ensure that appropriate guidance and training is given to the relevant staff, governors and other authorised school users on access to information procedures, records management and data breach procedures. Individuals will also be made aware and given training in relation to information security including using email and the internet.

The DPO will provide the School with adequate training resources and guidance materials. The DPO will be consulted, and will offer an adequacy opinion, if the School opts to use a third party training provider.

The School will maintain a 'training schedule' which will record when employees have completed an information governance training module and when a refresher is due to be completed.

The school will ensure that any third party contractors have adequately trained their staff in information governance by carrying out the appropriate due diligence.

PRIVACY NOTICES

The Joseph Rowntree School will provide a privacy notice to data subjects each time it obtains personal information from or about that data subject. Our main privacy notice will be displayed on the school's website in an easily accessible area. This notice will also be provided in a hard copy to pupils and parents at the start of their time at the School as part of their information pack.

A privacy notice for employees will be provided at commencement of their employment with the school. Specific privacy notices will be issued where the data subject requires more information about specific processing (e.g. school trips, projects).

Privacy notices will be cleared by the DPO prior to being published or issued. A record of privacy notices shall be kept on the school's Information Asset Register.

INFORMATION SHARING

In order to efficiently fulfil our duty of education provision it is sometimes necessary for the school to share information with third parties. Routine and regular information sharing arrangements will be documented in our main privacy notice (as above). Any adhoc sharing of information will be done in compliance with our legislative requirements.

DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

The school will conduct a data protection impact assessment for all new projects involving high risk data processing as defined by GDPR. This assessment will consider the privacy risks and implications of new projects as well as providing solutions to the identified risks.

The DPO will be consulted at the start of a project and will advise whether a DPIA is required. If it is agreed that a DPIA will be necessary, then the DPO will assist with the completion of the assessment, providing relevant advice.

RETENTION PERIODS

Retention periods will be determined by any legal requirement, best practice or national guidance, and lastly the organisational necessity to retain the information. In addition IAOs will take into account the Limitation Act 1980, which provides timescales within which action may be taken for breaches of the law, when determining retention periods.

The School has opted to adopt the retention schedule suggested by the Information and Records Maintenance Society (IRMS).

DESTRUCTION OF RECORDS

Retention periods for records are recorded in the school's IAR. When a record reaches the end of its retention period the IAO will arrange for the records, both electronic and paper to be

destroyed securely. Provisions to destroy paper information securely include cross cutting shredders and confidential waste bins. Advice in regards to the secure destruction of electronic media will be sought from relevant ICT support.

A record should be retained of all files destroyed including, where relevant:

- File reference number,
- Description of file,
- Date of disposal,
- Method of disposal,
- Officer who destroyed record

An Example Destruction Schedule can be found at Appendix 2.

THIRD PARTY DATA PROCESSORS

All third party contractors who process data on behalf of the school must be able to provide assurances that they have adequate data protection controls in place to ensure that the data they process is afforded the appropriate safeguards. Where personal data is being processed, there will be a written contract in place with the necessary data protection clauses contained.

Relevant senior leadership may insist that any data processing by a third party, ceases immediately if it believes that that third party has not got adequate data protection safeguards in place. If any data processing is going to take place outside of the EEA then the Data Protection Officer must be consulted prior to any contracts being agreed.

ACCESS TO INFORMATION

Requests for information under the Freedom of Information Act 2000 and Environmental Information Regulations 2004

Requests under this legislation should be made to the Headteacher who is responsible for:

- Deciding whether the requested information is held;
- Locating, retrieving or extracting the information;
- Considering whether any exemption might apply, the balance of the public interest test;
- Preparing the material for disclosure and drafting the response;
- Seeking any necessary approval for the response; and
- Sending the response to the requester

FOIA requests should be made in writing. Please note that we will only consider requests which provide a valid name and address and we will not consider requests which ask us to click on electronic links. EIR requests can be made verbally, however we will endeavour to follow this up in writing with the requestor to ensure accuracy.

Each request received will be acknowledged within 5 school days. The Chair of Governors and Headteacher will jointly consider all requests where a public interest test is applied or where there is any doubt on whether an exemption should be applied. In applying the public interest test they will:

- Document clearly the benefits of both disclosing or withholding the requested information;
- If necessary seek guidance from previous case law in deciding where the balance lies

- Consult the DPO

Reasons for disclosing or not disclosing will be reported to the next governing body meeting.

We have adopted the Information Commissioner's model publication scheme for schools and will publish as much information as possible on our website in the interests of transparency and accountability.

We will charge for supplying information at our discretion, in line with current regulations and following City of York Council's charging regime. If a charge applies, written notice will be given to the applicant and payment must be received before the information is supplied.
We will adhere to the required FOI/EIR timescales, and requests will be answered within **20 school days.**

Requests for information under the GDPR- Subject Access Requests

Requests under this legislation should be made to the Headteacher.

Any member of staff / governor may receive a request for an individual's personal information. Whilst GDPR does not require such requests to be made in writing, applicants are encouraged where possible to do so; applicants who require assistance should seek help from the school. Requests will be logged and acknowledged within 5 days.

We must be satisfied as to your identity and may have to ask for additional information such as:

- Valid Photo ID (driver's licence, passport etc);
- Proof of Address (Utility bill, council tax letter etc);
- further information for the school to be satisfied of the applicant's identity;

Only once the school is satisfied of the requestor's identity and has sufficient information on which to respond to the request will it be considered valid. We will then respond to your request within the statutory timescale of **1 calendar month**.

The school can apply a discretionary extension of up to a further 2 calendar months to comply with the request if the requested information would take a considerable amount of time to collate, redact, and prepare for disclosure due to either the complexity or voluminous nature of the records. If we wish to apply an extension we will firstly seek guidance from our DPO, then inform the applicant of the extension within the first calendar month of receiving the request. This extension period will be kept to a minimum and will not be used as a way of managing workloads. In very limited cases we may also refuse a request outright as 'manifestly unreasonable' if we would have to spend an unjustified amount of time and resources to comply.

Should we think any exemptions are necessary to apply we will seek guidance from our DPO to discuss their application.

If a subject access request is made by a parent whose child is 12 years of age or over we may consult with the child or ask that they submit the request on their own behalf. This decision will be made based on the capacity and maturity of the pupil in question.

All information being released should be handed over in person, sent securely via electronic means, or sent via recorded signed for delivery and stamped with a return address (in order of preference).

Requests received from parents asking for information held within the pupil's Education Record will be dealt with under the Education (Pupil Information) (England) Regulations 2005. Any charges which arise from this request will be applied at our discretion.

DATA SUBJECT RIGHTS

As well as a right of access to information, data subjects have a series of other rights prescribed by the GDPR including:

- Right to rectification
- Right to erasure
- Right to restrict processing
- Rights in relation automated decision making and profiling

All requests exercising these rights must be in writing and forwarded to the Headteacher who will acknowledge the request and respond within 1 calendar month. Advice regarding such requests will be sought from our DPO.

A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

COMPLAINTS

Complaints in relation to FOI/EIR and Subject Access will be handled through our existing Complaints Procedure. Any individual who wishes to make a complaint about the way we have handled their personal data should contact the DPO on the address provided.

COPYRIGHT

The Joseph Rowntree School will take reasonable steps to inform enquirers if any third party might have a copyright or intellectual property interest in information provided in response to their requests. However it will be the enquirer's responsibility to ensure that any information provided by the school is not re-used in a way which infringes those interests, whether or not any such warning has been given.

GENERAL

The Finance, Staffing and Resources Committee will be responsible for evaluating and reviewing this policy. The DPO will provide an annual GDPR compliance report for Governors that will be circulated to this committee for their review.

APPENDIX A – INFORMATION SECURITY INCIDENT REPORTING

This procedure has been written to inform The Joseph Rowntree School employees what to do if they discover an information security incident.

Any queries should be directed to the Data Protection Officer at SchoolsDPO@veritau.co.uk

Article 33 of the GDPR requires data controllers to report breaches of personal data to the Information Commissioner's Officer, and sometimes the affected data subject(s), within 72 hours of discovery if the incident is likely to result in a risk to the rights and freedoms of the data subject(s). Therefore it is vital that the School has a robust system in place to manage, contain, and report such incidents.

Notification and Containment

In order for the School to report serious incidents to the ICO within 72 hours it is vital that it has a robust system in place to manage, contain, and report such incidents.

Immediate Actions (within 24 Hours)

If an employee, governor or contractor is made aware of an actual data breach, or an information security event (a 'near-miss'), they must report it to their line manager and the School Business Manager (SBM) within 24 hours. If the SBM is not at work at the time of the notification then the Data Manager should be notified who will start the investigation process.

If appropriate, the person who located the breach, or their line manager, will make every effort to retrieve the information and / or ensure recipient parties do not possess a copy of the information.

Assigning Investigation (Within 48 Hours)

Once received, the SBM will assess the data protection risks and assign a severity rating according to the identified risks and mitigations. The severity ratings are graded as per the table below.

Rating	Incident Threshold	Recommended Actions
WHITE **Information Security Event**	No breach of confidentiality, integrity, or availability has taken place but there is a failure of the implemented safeguards that could lead to a breach in the future. *Examples* ▪ A post-it note containing a user name and password to a School database is found attached to a keyboard. ▪ A key safe, containing keys to filing cabinets, has been found unlocked and unsupervised.	▪ Responsible officer(s) spoken to by management and reminded of data protection responsibilities. If repeated offence management to consider HR action. ▪ Logged on school register of incidents
GREEN **Minimal Impact Incident**	The School's security measures have failed and have consequently resulted in a breach of confidentiality, integrity, or availability. Incident has been contained within the organisation (or trusted partner organisation). The information does not contain any special category data or any data that would be considered to be sensitive. The actual or potential detriment to individuals is virtually non-existent. *Examples* ▪ An email, containing details of a service user's address or contact details, is sent to an incorrect recipient within the School. ▪ A document containing the only record of pupil's contact details have been destroyed in error.	▪ Responsible officer(s) spoken to by management and reminded of data protection responsibilities. If repeated offence management to consider HR action. ▪ Logged on school register of incidents ▪ Notify SIRO ▪ Investigation report to be conducted by Information Asset Owner.

Rating	Incident Threshold	Recommended Actions
AMBER **Moderate Impact Incident**	The School's security measures have failed and have consequently resulted in a breach of confidentiality, integrity, or availability. The information has left school control. The information does not contain special category data or data that is considered to be sensitive but may contain data that should have been confidential to the School. The incident appears to affect only a small number of individuals. The actual or potential detriment is limited in impact and does not reach the threshold for reporting to the Information Commissioner's Office. *Examples* ▪ A letter is sent to the wrong postal address and the incorrect recipient has learnt of another individual's dealings with the School. However, the letter does not contain any special category information. ▪ An email has been sent to ten parents without the BCC function being utilised which reveals all ten personal email addresses.	▪ Responsible officer(s) asked to re-sit Data Protection e-learning. Management to consider HR action. ▪ Consider utilising key messages/intranet to remind all staff of certain data protection best practice. ▪ Logged on School register of incidents ▪ Notify SIRO ▪ Investigation report to be conducted by Information Asset Owner.
RED **Serious Impact Incident**	The School's security measures have failed and have consequently resulted in a breach of confidentiality, integrity, or availability. The information has left school control. The information contains special category data or data that is considered to be sensitive in nature and/or affects a large number of individuals. The incident has or is likely to infringe on the rights and freedoms of an individual and has a likely potential to cause detriment (emotional, financial, or physical damage) to individuals. *Examples* ▪ A file, containing safeguarding and health data, is left unsupervised in a vehicle which is subsequently stolen and the data has been lost to persons unknown. ▪ A spreadsheet containing the SEN information for all the School's pupils has been mistakenly sent to a member of the public.	▪ Management to consider (potentially immediate) HR action. ▪ Logged on school register of incidents ▪ Notify SIRO and Data Protection Officer ▪ Consider forming an incident strategy conference ▪ Consider reporting to the ICO ▪ Consider informing affected individual(s) ▪ Consider informing the police or other law enforcement agencies. ▪ Where appropriate the Data Protection Officer to conduct incident investigation with assistance (where and if required) from internal audit and counter fraud colleagues.

The SBM will notify the Headteacher and the relevant Information Asset Owner (IAO) that the breach has taken place. The SBM will recommend immediate actions that need to take place to contain the incident.

The IAO will investigate white, green and amber incidents. Red incidents will be investigated by the Data Protection Officer with the assistance of Internal Audit and Counter Fraud Teams.

Reporting to the ICO/Data Subjects (Within 72 Hours)

The Headteacher, in conjunction with the SBM, IAO and DPO will make a decision as to whether the incident needs to be reported to the ICO, and also whether any data subjects need to be informed. The IAO will be responsible for liaising with data subjects and the DPO for liaising with the ICO.

Investigating and Concluding Incidents

The SBM will ensure that investigations have identified all potential information risks and that remedial actions have been implemented.

When the DPO has investigated a data breach then the Headteacher must sign off the investigation report and ensure recommendations are implemented.

The Headteacher will ensure all investigations have been carried out thoroughly and all highlighted information security risks addressed.

APPENDIX B – EXAMPLE DESTRUCTION SCHEDULE

#	Name of Information	Data Information Created (or range of dates)	Asset Owner and Job Title	Description of information (what was purpose etc)	Format (electronic / paper etc)	Retention Period	Who has access to / uses the information	Date Destroyed	Method of destruction	Name of staff (and job title) who deleted data	Authorised by Information Asset Owner?	Comments/ Notes
1	*eg List of pupils on Free School meals*	*Sept 2007 - 2008*	*Headteacher / Deputy Headteacher etc*	*eg correspondence about, list of pupils, pupil info, dietry requirements for the purpose of...*	*Electronic*	*10 years*	*Admin Staff Only*	*10-Sep-18*	*Deleted from School systems*		*Y*	