Rumworth School

Information Management Policy for Maintained Schools

Rumworth School

The school is a public authority and has a number of legal responsibilities for the management of information.

This document is designed to provide a framework for both the school and its members of staff to fulfill their duties around the collection, handling, storage, retention and security of information. It should be read in conjunction with the associated retention schedule for advice on how long to keep data.

Amendment History

Version / Issue No.	Date	Author	Remarks / Reason for Change
V.01	02.11.2012	Paul Rankin	
V 02	14.04.2014	Tasadiq Naveed	
V 03	05.03.2015	Tasadiq Naveed	
V 04	02/05/2018	Ann McDonna	Update policy with GDPR
	August 2018	H Lane	Adapted to suit Rumworth School
	November 2018	H Lane	Reviewed prior to Governor approval Moved retention schedule to separate document

The General Data Protection Regulation (GDPR) and the Data Protection Bill

The General Data Protection Regulation (GDPR) is a Europe-wide law which is part of a wider package of reform intended to modernise data protection laws.

The Data Protection Act 1998 was introduced to protect the individual rights and freedoms of individuals, especially their right to privacy with respect to the processing of personal data. GDPR builds on this legislation, enhancing information rights for the public and placing a much greater emphasis on organisations being able to show how they comply with the data protection principles, for example by having effective policies and procedures in place, and documenting and demonstrating their accountability.

GDPR applies to all personal data, regardless of whether it is held electronically (on a computer system, in emails, in text messages etc.) or on paper. There are particularly stringent rules surrounding "special category" data (similar to 'sensitive' data in the Data Protection Act 1998) such as pupil identifiers, pupil characteristics, special educational needs, health, religious beliefs, ethnic background, home address and biometric data. In addition GDPR explicitly states that children's personal data merits specific protection.

GDPR also introduces new responsibilities around the collection and use of pseudonymised personal data (data where any identifying characteristics have been replaced with a pseudonym (or value) that means that the data subject cannot be directly identified, but they can be identified by indirect means such as using underlying or related data. For example: where an individual is allocated a client reference which is used instead of their name.)

As part of the reform of data protection laws, the Data Protection Bill, published on 14th September 2017, is currently being considered by Parliament and once passed will repeal the Data Protection Act 1998. As GDPR and the Data Protection Bill complement each other it is important that they are read side by side.

Rumworth School is registered with the Information Commissioner's Office as a Data Controller and aims to fulfil its obligations to the fullest extent and to comply with the six data protection principles set out in the GDPR which require that personal data is:

1. Processed lawfully, fairly and transparently
2. Collected for a specified, explicit and legitimate purpose
3. Adequate, relevant and limited to what is necessary (ie: proportionate) for the purpose it is being processed
4. Accurate and kept up to date, with every reasonable step taken to erase or rectify inaccurate personal data without delay
5. Held in a form that means the data subject can be identified for only as long as is necessary for the purpose for which the personal data is processed
6. Processed in a manner that ensures appropriate security of the personal data

Processing Personal Data

Before processing personal data the school will first identify a legal basis for doing so. When processing special category data the school will also satisfy one of the special category conditions.

Details of the legal bases, special categories of data and the special category conditions can be found in Appendix 1.

Privacy Notice - Fair Processing of Data

Under principle 4 of the GDPR, the school has a duty to check that children, parents and carers information is accurate and up to date. It fulfils this by sending out a data collection form to parents/carers on an annual basis. This form will also include a privacy notice which outlines to the parent/carer:

- What information is held
- Why the information is held
- How long the information is held
- Who the information is shared with
- How children, parents and carers can access the information which is held about them

An updated privacy notice for pupil data is available for the school.

The school also has a duty to check that staff information is accurate and up to date. It fulfils this by asking staff to complete a data collection form. The form will also include a privacy notice which will outline:

- What information is held
- Why the information is held
- How long the information is held
- Who the information is shared with
- How staff can access the information which is held about them

An updated privacy notice for staff data is available for the school.

Consent

Consent is one of the legal bases available to the school, although this will only be used where there is no other legal basis available.

Where the school is relying on consent to process personal data, this will be proactive, made clear to the data subject and will be separate from other matters. It will also be made clear that consent can be withdrawn at any time and the method to do so will be clear and accessible; it will be as easy to withdraw consent as it was to give consent.

If consent is withdrawn, the school will immediately cease processing the personal data.

There are additional provisions within GDPR regarding securing consent from children. When offering an online service directly to a child, only children aged 13 or over are able provide their own consent. (This is the age proposed in the Data Protection Bill and is subject to Parliamentary approval). For younger children, consent would need to be provided by whoever holds parental responsibility for the child (unless the online service offered is a preventive or counselling service). In such cases, the school will make reasonable efforts to verify that consent is given or authorized by a parent or guardian.

A separate Privacy Notice will be issued to children and will written in clear and age appropriate language.

Information Security

Under principle 6 of the GDPR, the school has a duty to ensure that data is handled securely. To fulfill its obligations under the act and to comply with Cabinet Office guidelines outlined in "Data Handling Procedures in Government" the school will adopt the following to maintain data security:

- Users may not remove or copy sensitive or personal data from the school or authorised premises unless the media is encrypted and is transported securely for storage in a secure location.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Sensitive or personal data must be securely deleted when it is no longer required.
- Computer passwords should not be disclosed or shared between users
- Files and paperwork that identifies individuals must never be left unattended and must be stored in locked cabinets within a controlled access room that must be

locked when not in use

- All staff processing personal information should be appropriately trained

The school will use a protective marking scheme to ensure that all data – electronic or on paper – is labelled according to the protection it requires based on Impact Levels:

Impact level	Colour Code	Memory stick?	Example
IL0– Not Protectively Marked		Yes	Newsletters, public information
IL1- Unclassified		Yes	Generic letters to parents containing no personal data
IL2–PROTECT		No	Basic student information such as name and address
IL3–Restricted		No	Sensitive Student information such as ethnicity or FSM status
IL4-Confidential		No	Highly sensitive student data relating to child protection

Information Asset Register and Record of Processing Activity

An information asset register will be compiled and kept up to date. This will summarise each information asset the school maintains and include a record of activities related to higher risk processing such as processing personal data that could result in a risk to the rights and freedoms of individuals, and the processing of special category data, or criminal convictions / offences.

Appropriate measures will be taken to mitigate the risk of disclosure of each information asset based on the impact level assigned.

The information documented in the information asset register must reflect the current situation as regards the processing of personal data and therefore will be regularly reviewed to ensure that it remains accurate and up to date.

Data Protection Impact Assessments

In order to ensure that all data protection requirements are identified and any associated risks are addressed, the school will complete a Data Protection Impact Assessment (DPIA) (previously known as a privacy impact assessment (PIA)) when introducing a new, or revising an existing, system or process which involves processing personal data.

Data Protection Officer

As a public authority, the school has a duty under GDPR to appoint a Data Protection Officer to assist with monitoring internal compliance, inform and advise on the school's data protection obligations and provide advice regarding Data Protection Impact Assessments (DPIAs).

The DPO will be independent, an expert in data protection, adequately resourced, and report to the highest management level.

Incident Reporting

GDPR introduces a legal duty to report certain types of personal data breach to the Information Commissioner's Office (ICO); this must be done **within 72 hours** of the school becoming aware of the breach, where feasible, even if all details of the breach are not yet known.

In addition, the school is required to inform the data subjects of the breach without undue delay if it is considered that there is a high risk of the breach adversely affecting their rights and freedoms.

In order to meet these requirements, any suspected and/or actual breaches of information security will be reported to the school's Data Protection Officer immediately, and in any event **within 24 hours** of the school becoming aware of the breach, using the form attached at Appendix 3.

Records will be maintained of any suspected breaches of information security using this form. The details of the incident will be used to determine whether the breach requires a report to the ICO and/or the data subjects, and, following investigation, to create a correctional plan to ensure that a similar incident does not happen.

Record Retention

The school maintains a records management policy which details compliance with the Lord Chancellor's Code of Practice which can be found here:
http://www.justice.gov.uk/downloads/information-access-rights/foi/foi-section-46-code-of-practice.pdf

A detailed retention schedule and protective marking scheme is outlined in the additional document 'Retention of Records-Rumworth School'

This retention schedule is based on guidance from the records management society: http://www.irms.org.uk/images/resources/infoguides/records_management_toolkit_for_schools_version_4_may_2012.pdf

It encompasses records managed by all types of school – some of the file descriptions listed may not be relevant to every school.

Regarding documents marked as offer or transfer to Archive, it would be the school's responsibility to contact Bolton Archives service on 01204 333173 or e-mail libraries@bolton.gov.uk

**Please note that retaining documents beyond their retention or transfer dates may breach principle 5 of the -GDPR

The Right to be Forgotten

Under GDPR individuals have the right to have personal data erased, this is also known as the 'right to be forgotten'. There is a particular emphasis on the right to erasure if the request relates to data collected from children. The right to be forgotten is not absolute and only applies in certain circumstances.

An individual can make a request for data to be erased either verbally or writing. The school will respond to such requests within 1 calendar month to advise of its decision and will provide a clear justification if it refuses the request.

If personal data which the school has shared with others is erased, the school will inform each recipient of the erasure, unless this proves impossible or involves disproportionate effort.

Disclosure of personal information

Personal information will be disclosed to 3rd parties under the following conditions:

Information sharing with professionals working with children

Information sharing between professionals is vital to ensure the wellbeing of Children. The school will follow the "7 golden rules of Information Sharing" described by the DfE:

1. Remember that GDPR is not a barrier to sharing information
2. Be open and honest with the person or family
3. Seek advice if you are in any doubt
4. Share with consent where appropriate
5. Consider safety and well-being
6. Necessary, proportionate, relevant, accurate timely, and secure
7. Keep a record of your decision and reasons

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/277834/information_sharing_guidance_for_practitioners_and_managers.pdf

Unauthorised disclosure of personal data is a criminal offence under Section 55 of the Data Protection Act 1998 and will likely lead to disciplinary action

Investigation of a crime

(Please note that Section 3 of the Data Protection Bill sets out specific data protection principles to be considered when processing personal data for law enforcement purposes. This section of the policy will therefore be refreshed at such time as the Bill is passed and becomes UK law)

The school will treat requests for information from an official bodies related to criminal or taxation purposes under Sections 28, 29 and 35 of the Data Protection Act 1998. The school requires the requestor to complete the Request for personal data form (Appendix 4).

Under section 29 requests from the police will be countersigned by a person no lower than inspector. For requests from other organisations other than the police, the form will be countersigned by a person of a higher position within the organisation than the person making the request.

Generally, the school reserves the right not to release the data but there may be situations such as the receipt of a court order that requires the school to release the information.

Access to Pupils' Records

There are two distinct rights to information held by schools about pupils.

1. Subject Access Right – under GDPR a pupil has the right to a copy of their information; this type of request is a Subject Access Request (SAR). In certain circumstances requests may be made by a parent on behalf of the child.

2. Rights to the educational record – under the Education (Pupil Information) (England) Regulations 2005, a parent has the right to access their child's educational record.

Subject Access Requests – a child or young person will always be the owner of their personal information as defined within the GDPR. However, if a young person is incapable of making their own decisions, which needs to be assessed on a case by case basis, but is generally accepted as being under the age of 12 years, the primary carer or guardian would act on their behalf. This authority is only extended to functions that are in the best interests of the child or young person.

The school will respond to the request within 1 calendar month of receipt; this may be extended by up to 2 further calendar months if a request is complex, in which case the school will contact the requester within 1 calendar month of receipt and explain why the extension is necessary.

Education (Pupil Information) (England) Regulations 2005 – requests from parents to view their child's educational record will be dealt with by the Board of Governors. The request must be made in writing and a response must be provided within 15 school days.

The pupil cannot prevent a parent from accessing their educational record under the Pupil Information Regulations, but they can object to their parent accessing information through a Subject Access Request, assuming that the child in question is sufficiently mature to make such a decision.

The Protection of Freedoms Act 2012

The Protection of Freedoms Act was introduced in February 2011 and came into force on 9th May 2012 with the commencement orders coming into force in July 2012. It is an Act to impose consent and other requirements in relation to processing of biometric information relating to children, to provide a code of practice about surveillance camera systems amongst other things.

CCTV AND OTHER SURVEILLANCE CAMERA TECHNOLOGY

CCTV surveillance has become a common feature of our daily lives and now there is an increasing use of these in and around educational settings. Information held by the school is covered under GDPR; capture of CCTV must be in line with relevant codes of practice including the Surveillance Camera Code of Practice issued by the Surveillance Camera Commissioner, available here:
https://www.gov.uk/government/publications/surveillance-camera-code-of-practice
and the CCTV Code of Practice issued by the Information Commissioner's Office, available here
:https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Recorded material will be stored in a way that maintains the integrity of the image. Once there is no reason to retain the recorded images, **they will be deleted**.

In area where CCTV surveillance is being carried out there will be clear markings to reflect this.

Subject access requests for CCTV images

Individuals whose images are recorded have a right to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images. This will be provided within 1 calendar month of receiving a request.

BIOMETRIC DATA

RUMWORTH SCHOOL DOES NOT CURRENTLY COLLECT, USE OR STORE BIOMETRIC DATA

Disclosure of non - personal information / FOI Requests

The school as a public authority is subject to The Freedom of Information Act 2000 and all requests for information that is not personal information must be treated as a Freedom of Information request. FOI requests must be fully responded within 20 (school) working days by law. The information will be provided unless the school can provide an exemption under the FOI act

A more detailed guide to FOI exemptions is here:
https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

https://ico.org.uk/media/for-organisations/documents/1643/foi_hints_for_practitioners_handing_foi_and_eir_requests_2008.pdf

Roles and Responsibilities

The senior information risk owner (SIRO) for the school is Gary Johnson, Head Teacher

They are responsible for:

- Owning and updating this policy
- Owning the information risk register
- Appointing Information Asset Owners (IAOs) for each Information Asset
- Advocating information risk management and raising awareness of information security issues
- After liaising with the Data Protection Officer, determining whether a security incident is of sufficient severity to report to the Information Commissioner's Office, and if the risk of adverse impact on the data subject(s) is such that they should be notified

The Data Protection Officer for the school is Judith Smith (dpo**@**manchester.gov.uk)

They are responsible for:

- Informing and advising on the school's obligations to comply with GDPR and other data protection laws
- Monitoring compliance with GDPR and other data protection laws
- Monitoring compliance with the school's data protection policies and procedures, including managing internal data protection activities, raising awareness of data protection issues, training staff and conducting internal audits
- Advising on and monitoring Data Protection Impact Assessments
- Acting as first point of contact for individuals whose data is process (pupils, parents, employees etc) and for the Information Commissioner's Office, and any other relevant supervisory authorities.

Information Asset Owners are responsible for:

- Ensuring the information is used for the purpose it was collected
- How information has been amended or added to over time
- Who has access to protected data and why

All staff are responsible for ensuring that information is managed according to this policy.

Signed on behalf of the Governing body:

Signed _____ Date_____

Chairperson of the Governing body

Appendix 1

Processing Personal Data: Legal Basis, Special Category Data and Special Category Conditions

Legal Basis: The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

d) **Vital interests:** the processing is necessary to protect someone's life.

e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Special Category Data: GDPR identifies that some information is particularly sensitive and therefore needs extra protection:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership Health
- Sexual life or orientation
- Genetic data (e.g. blood samples DNA)
- Biometric data to identify an individual (e.g. finger-prints, iris recognition)
- Financial information

Special Category Conditions: Under GDPR if you are processing special category data you need to meet a special category condition in addition to the legal basis identified above. The special category conditions are:

- The data subject has given explicit consent

- Necessary to protect the vital interests where the data subject is physically or legally incapable of giving consent
- The data has been made publically available by the data subject
- Necessary for the purposes of preventative or occupational medicine, for example the assessment of the working capacity of an employee
- Required for exercising rights in the field of employment and social security or social protection
- Processing is carried out by a foundation or not-for-profit body in the course of its legitimate activities
- Necessary to process legal claims
- Necessary for archiving statistical or historical research which is in the public interest
- Necessary for reasons of substantial public interest on the basis of UK law which shall be proportionate to the aim pursued

Data relating to criminal convictions or offences: Under GDPR information relating to criminal convictions (includes all DBS checks even if they show no convictions/offences) can only be processed process if you are doing so in an official capacity or have specific legal authorisation to do so.

(Please note that Section 3 of the Data Protection Bill sets out specific data protection principles to be considered when processing personal data for law enforcement purposes. This section of the policy will therefore be refreshed at such time as the Bill is passed and becomes UK law)

Appendix 2

Information Security Incident Report Form

All boxes must be completed

Rumworth School

To be completed by the person reporting the breach

Name	
Job title	
Department / Section (if applicable)	
Telephone number	
E-mail address	
Date	
What has happened? Please provide as much information as you can about what has happened, what went wrong and how; include a description of the data, eg: format, volume, from which system, and the location of the breach.	
How did you find out about the breach? If you were not the person who originally found there had been a breach, please explain how you found out about it and how they found out about it.	
Was the breach caused by a cyber incident?	

Yes		**No**		**Not yet known**	

When was the breach discovered?	**Date:**		**Time:**	
When did the breach occur?	**Date:**		**Time:**	
What has happened to the information? (Please select all that apply)				

Destroyed		**Lost**		**Stolen**	
Altered		**Unauthorised Disclosure**		**Unauthorised Access**	

Other (please give details below)	

Categories of personal data included in the breach (Please select all that apply)			
Basic personal identifiers (eg: name, contact details)		**Identification data (eg: usernames, passwords)**	
Racial or ethnic origin		**Political opinions**	
Religious or philosophical beliefs		**Trade union membership**	
Health		**Sexual life or orientation**	
Gender reassignment data		**Genetic or biometric data**	
Financial information		**Criminal convictions or offences**	
Official documents (eg: driving licences)		**Location data**	
Other (please give details below)		**Not yet known**	

How many data subjects could be affected?	

Categories of data subjects affected (Please select all that apply)			
Employees		**Pupils**	
Parents / Carers		**Governors**	
Volunteers		**Other (please give details below)**	

What is the possible impact of the breach on the data subjects?

Has there been any actual harm to data subjects? (If yes, please give details below)					
Yes		**No**		**Not yet known**	

What is the likelihood that data subjects will experience significant consequences as a result of the breach? (Please select one option and give further details below)					
Very likely		**Likely**		**Neutral**	
Unlikely		**Very unlikely**		**Not yet known**	

Have you told the data subjects about the breach?			
Yes		**About to or in process of telling them**	
No, but they're already aware		**No, but planning to tell them**	
No, decided not to tell them		**Not yet decided whether to tell them**	
Seeking advice from DPO		**Other (Please give details below)**	
Have you told, or are you planning to tell, any other organisations (e.g. police, regulatory body) about the breach? (If yes, please give details below. If you have a crime reference number, please include it)			
Yes		**No**	
Seeking advice from DPO		**Other (Please give details below)**	
What measures have been taken to deal with the breach? (e.g. contacting the person sent in formation in error, auto-erased lost laptop)			
Has the data been recovered? (Please give details - if the breach is due to a misdirected email, include whether you have had confirmation that the recipient has deleted it and whether it was read or unread)			
Yes		**No**	
What measures have been taken / are proposed to mitigate further breaches?			
If there is any further information you think should be considered please include it here.			

To be completed by the Data Protection Officer

Form received by DPO	**Date:**		**Time:**			
Was the form received within 24 hours of the breach being discovered?			**Yes**		**No**	
If no, was a reason given? (Please give details below)			**Yes**		**No**	
Is the information on the form complete?			**Yes**		**No**	
If not, what further information is required? (Please give details below)						

Breach reported to SIRO	**Yes**		**No**		**Date**	
Breach reported to Head Teacher	**Yes**		**No**		**Date**	
Breach reported to Chair of Governors	**Yes**		**No**		**Date**	

What measures have been agreed should be taken to deal with the breach?
What measures have been agreed should be taken to mitigate harm caused by the breach?

Have data subjects been told about the about the breach (if not already done by person reporting it)?			
Yes		**About to or in process of telling them**	
No, but they're already aware		**No, but planning to tell them**	
No, decided not to tell them		**Other (Please give details below)**	

Does the breach warrant a report to the ICO?	**Yes**		**No**	
If yes, when was the breach reported to the ICO?	**Date:**		**Time:**	
Was report to ICO made within 72 hours?	**Yes**		**No**	
If report was not made within 72 hours, please provide justification for late reporting below.				
What has been identified as the root cause(s) of the breach following investigation?				
What corrective actions have been identified following investigation?				

Action	Target Date	Owner	Date Completed

DPO Sign-off		**Date**	
Head Teacher Sign-off		**Date**	
Date Incident Investigation Closed			

Appendix 3

Request for personal data Form

Request for personal data

All boxes must be completed

Rumworth School

To

Details of applicant

Name of applicant	
Job title	
Department and Section	
Full Address	
Telephone number	
e-mail address or fax number	
Investigation reference / Operation Name	
Date	

Details of application

1. **This request is made pursuant to the Data Protection Act 1998. I can confirm that this request complies with the following non-disclosure provisions**

Section 29

☐ The data is necessary for the prevention or detection of crime

☐ The data is necessary for the apprehension or prosecution of offenders

Section 35

☐ The data is necessary for the purpose of or in connection with present legal Proceedings

☐ The data is necessary for the purpose of or in connection with prospective legal proceedings

2. **I require the following information**

3. **Why I require the information**
4. **What statutory powers does the requester have to demand the information**
5. **I can confirm that the information you provide will be held in the strictest confidence and will not be further processed beyond the purpose for which it was requested.** **I have grounds believing that failure to disclose the required information will be likely to prejudice my enquiries and can confirm that the details supplied on this form are, to the best of my knowledge, correct.** **I am aware of the provisions of Section 55 of the Data protection Act 1998, regarding the unlawful obtaining of personal details.**
Signature Print Name