ROYSTON SCHOOLS ACADEMY TRUST

Data Protection Policy

Policy review:		**Sept 2018**
Reviewed by:		RSAT Board
Ratified by:		RSAT Board
Next Review:		Sept 2019
Statutory Document:	Y	
Update on Website:	Y	
Additional Comments:	Royston Schools Academy Trust (RSAT) encompassess Meridian Upper School, Greneway Middle School and Roysia Middle School. This policy will be reviewed every two years, unless guidance from HfL or DfE is received. From May 2018, schools must ensure their data processing complies with new data protection law under the General Data Protection Regulation (GDPR) and this policy will be reviewed upon guidance from DfE	

Data Protection Policy and Toolkit

Schools handle increasing amounts of personal information and have a statutory requirement to comply with The Data Protection Act 1998 ("DPA"). From May 2018 they must comply with the General Data Protection Regulation ("GDRP"). Schools should have clear policies and procedures for dealing with personal information, and be registered with the Information Commissioner's Office ("ICO"). Schools should have systems in place to reduce the chances of a loss of personal information, otherwise known as a data breach which could occur as a result of theft, loss, accidental disclosure, equipment failure or hacking.

Contents

The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- The law regarding personal data
- How personal data should be processed, stored, archived and deleted/destroyed
- How staff, parents and pupils can access personal data

1.1. It is a statutory requirement for all schools to have a Data Protection Policy:
(http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools)

1.2. Data Protection Principles

The Data Protection Act 1998 establishes eight principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Article 5 of the GDPR requires that personal data shall be:
(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be 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;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

1.3 Individual's' rights

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA.

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

2. Data Types

Not all data needs to be protected to the same standards, the more sensitive or potentially damaging the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. In a school environment staff are used to managing risk, for instance during a PE or swimming lesson where risks are assessed, controlled and managed. A similar process should take place with managing school data. The DPA defines different types of data and prescribes how it should be treated.

The loss or theft of any Personal Data is a “ Potential Data Breach” which could result in legal action against the school. The loss of sensitive personal data is considered much more seriously and the sanctions may well be more punitive.

2.1. Personal data

RSAT will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:-

- Personal information about members of the school community – including pupils / students, members of staff and parents / carers eg names, addresses, contact details, legal guardianship contact details, disciplinary records.
- Curricular / academic data eg class lists, pupil / student progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records, disciplinary records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

2.2. Sensitive Personal data

Sensitive personal data is defined by the Act as information that relates to the following 8 categories: race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexual life and criminal offences, criminal proceedings. It requires a greater degree of protection and in a school would include:-

- Staff Trade Union details
- Information on the racial or ethnic origin of a child or member of staff
- Information about the sexuality of a child, his or her family or a member of staff
- Medical information about a child or member of staff
- Information relating to any criminal offence of a child, family member or member of staff.

Note – On some occasions it is important that medical information should be shared more widely to protect a child - for instance if a child had a nut allergy how it should be treated. Where appropriate written permission should be sought from the parents / carers before posting information more widely, for instance in the staff room.

2.3. Other types of Data not covered by the act.

This is data that does not identify a living individual and therefore is not covered by the remit of the DPA this may fall under other access to information procedures. This would include Lesson Plans (where no individual pupil is named), Teaching Resources, and other information about the school which does not relate to an individual. Some of this data would be available publically (for instance the diary for the forthcoming year), and some of this may need to be protected by the school (If RSAT has written a detailed scheme of work that it wishes to sell to other schools). RSAT may choose to protect some data in this category but there is no legal requirement to do so.

The ICO provide additional information on their website See
http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

3. Responsibilities

RSAT are responsible for Data Protection, they may appoint a DPO to manage data.

3.1. Risk Management - Roles

The Trust's Data Protection Officer **(DPO)** is Mr Gordon Farquhar. This individual will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners **(IAOs**)

RSAT will identify Information Asset Owners (IAOs) in each school for the various types of data being held (e.g. pupil / student information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand :

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to protected data and why.

3.2. Risk management - Staff and Governors Responsibilities

- Everyone in the school has the responsibility of handling personal information in a safe and secure manner.

- Directors/Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Director/Governor.

4. Legal Requirements

4.1. Registration

Each school within RSAT must be registered as a Data Controller on the Data Protection Register held by the Information Commissioner and each school is responsible for their own registration): http://ico.org.uk/for_organisations/data_protection/registration

4.2. Information for Data Subjects (Parents, Staff)

In order to comply with the fair processing requirements of the DPA, the Trust will inform parents / carers of all pupils / students and staff of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through a letter via their websites. More information about the suggested wording of privacy notices can be found on the DfE website:
http://www.education.gov.uk/researchandstatistics/datatdatam/a0064374/pn

See Appendix 2

5. Transporting, Storing and Deleting personal Data

- The policy and processes of the Trust will comply with the guidance issued by the ICO here

5.1. Information security - Storage and Access to Data

5.1.1. Technical Requirements

- RSAT will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled

according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (ie owned by the users) must not be used for the storage of personal data.

- Each school has a clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

5.1.2. Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected),
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

5.1.3. Passwords

- All users will use strong passwords which must be changed regularly. User passwords must never be shared. It is advisable NOT to record complete passwords, but prompts could be recorded.

5.1.4. Images

- Images of pupils will only be processed and transported by use of encrypted devices and permission for this will be obtained in the privacy agreement.
- Images will be protected and stored in a secure area.

5.1.5. Cloud Based Storage

- Each school within RSAT has clear policy and procedures for the use of “Cloud Based Storage Systems” (for example dropbox, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

5.2. Third Party data transfers

- As a Data Controller, RSAT is responsible for the security of any data passed to a “third party”. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party. http://ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

5.3. Retention of Data

- The guidance given by the Information and Records Management Society – Schools records management toolkit will be used to determine how long data is retained.
- Personal data that is no longer required will be destroyed and this process will be recorded.

5.4. Systems to protect data

5.4.1. Paper Based Systems

- All paper based OFFICIAL or OFFICIAL – SENSITIVE (or higher) material must be held in lockable storage, whether on or off site.
- Paper based personal information sent to parents will be checked by a member of the senior management team before the envelope is sealed.

5.4.2. School Websites

- Uploads to the school website will be checked prior to publication ensure that personal data will not be accidentally disclosed and that images uploaded only show pupils where prior permission has been obtained

5.4.3. E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data.

- E-mails containing sensitive information should be encrypted, for example by attaching the sensitive information as a password protected word document. The recipient will then need to contact the school for access to a one-off password

Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information.

- In the event of a data breach the SIRO will inform the head teacher and chair of governors

Appendix 1 Links to resources and guidance

ICO Guidance for schools
http://ico.org.uk/for_organisations/sector_guides/~/media/documents/library/Data_Protection/Research_and_reports/report_dp_guidance_for_schools.ashx
A downloadable guide for schools

Overview of the General Data Protection Regulation (GDPR)
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Specific information for schools is available here
http://ico.org.uk/for_organisations/sector_guides/education

Specific information about use of Cloud Based technology
http://ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing

Specific Information about CCTV
http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv

Information and Records Management Society – Schools records management toolkit
http://www.irms.org.uk/resources/information-guides/199-rm-toolkit-for-school
A downloadable schedule for all records management in schools

Disclosure and Barring Service (DBS)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/143669/handling-dbs-cert.pdf Details of storage and access to DBS certificate information.

DFE Privacy Notices
https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

DFE Use of Biometric Data
https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

Appendix 2 Privacy Notices

These are now separate attachments which are drawn from:
www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

Appendix 3 Glossary

Data Protection Act 1998: All personal data which is held must be processed and retained in accordance with the eight principles of the Act and with the rights of the individual. Personal data must not be kept longer than is necessary (this may be affected by the requirements of other Acts in relation to financial data or personal data disclosed to Government departments). Retention of personal data must take account of the Act, and personal data must be disposed of as confidential waste. Covers both personal data relating to employees and to members of the public.

ICO The Information Commissioner's office. This is a government body that regulates the Data Protection Act.
The ICO website is here http://ico.org.uk/

Data Protection Act 1998: Compliance Advice. Subject access – Right of access to education records in England: General information note from the Information Commissioner on access to education records. Includes timescale (15 days) and photocopy costs.

Data Protection Act 1998: Compliance Advice. Disclosure of examination results by schools to the media: General information note from the Information Commissioner on publication of examination results.

The General Data Protection Regulation 2018: The GDPR applies to 'controllers' and 'processors'. The definitions are broadly the same as under the DPA – ie the controller says how and why personal data is processed and the processor acts on the controller's behalf. If you are currently subject to the DPA, it is likely that you will also be subject to the GDPR.

Education Act 1996: Section 509 covers retention of home to school transport appeal papers. (By LA)

Education (Pupil Information) (England) Regulations 2005: Retention of Pupil records

Health and Safety at Work Act 1974 & Health and Safety at Work Act 1972: Retention requirements for a range of health and safety documentation including accident books, H&S manuals etc.

School Standards and Framework Act 1998: Retention of school admission and exclusion appeal papers and other pupil records.

Appendix 4 Check Sheet

Schools may find it beneficial to use this to check their systems for handling data.

- Training for staff on Data Protection, and how to comply with requirements
- Data Protection Policy in place
- All portable devices containing personal data are encrypted
- Passwords – Staff use complex passwords
- Passwords – Not shared between staff
- Privacy notice sent to parents
- Privacy notice given to staff
- Images stored securely
- School registered with the ICO as a data controller
- Member of staff with overall responsibility for data identified (SIRO)
- Risk assessments complete
- Systems in place to ensure that data is retained securely for the required amount of time
- Process in place to allow for subject access requests.
- If school has CCTV appropriate policies are in place to cover use, storage and deletion of the data, and appropriate signage is displayed
- Paper based documents secure
- Electronic backup of data both working and secure
- Systems in place to help reduce the risk of a data breach *e.g. personal data sent out checked before the envelope sealed, uploads to websites checked etc*