Data Protection Policy

Independent Boarding and Day School for Boys and Girls
Royal Hospital School

May 2018

ISI reference	N/A
Key author	Director of Finance and Operations (Bursar)/Privacy and Compliance Officer
Reviewing body	SMT
Approval body	Risk and Audit Committee
Approval frequency	2 years
Last approved	15th May 2018
Related Policies	• RHS Privacy Notice • Additional Privacy Notices – RHS EL, RHS CT, Music At RHS, Staff and New Applicants, Contractors, Pupils, School website • Data Documentation, Information Security and Retention Policy • Taking, Storage and Using Images of Children Policy • Acceptable Use Policy • CCTV Policy • Admissions Policy and Procedure • Parent Registration, Parent Contract • Pupil Digital Handbook • On Line Safety Policy

1. Background

UK Data Protection Law consists of the following elements:

- prior to 25 May 2018, the Data Protection Act 1998;
- from 25 May 2018, the General Data Protection Regulation (EU 2016/679) (GDPR) and any legislation which amends, re-enacts or replaces it in England and Wales;
- the Electronic Communications (EC Directive) Regulations 2003, together with any legislation which replaces it; and
- at all times, any other data protection laws and regulations applicable in England and Wales.

The overall intent of GDPR is to strengthen and unify data protection for all individuals. Key elements include:

- New rights for individuals in relation to their data, including children.
- More specific criteria for the requirement for consent and how it's obtained.
- Increased requirements around record keeping and reporting.
- Application of Data Privacy Impact Assessments (DPIAs) to new technology/procedures.
- Increased information security.
- Requirement to include additional information in privacy notices and contracts with data processors.

In the UK, the regulating authority is the Information Commissioner's Office (ICO). Organisations can be heavily fined for serious compliance infringements such as:

- Not having sufficient consent to process individuals' data when consent is required.
- Not having records in order.
- Not notifying the ICO of a breach, or delay beyond 72 hours.

The Royal Hospital School (RHS) operates as part of Greenwich Hospital (GH), and has no separate legal identity from GH. The School has therefore sought to meet GH's GDPR compliance and liability requirements as well as taking guidance from the ICO and the Independent Schools Bursars Association (ISBA) and their legal advisers.

Independent schools are not subject to the specific information provisions (including the parental right to see the pupil record, and Freedom of Information) that will be applicable to maintained schools under separate legislation. In addition, while maintained schools are public authorities and hence strictly required to appoint a Data Protection Officer (DPO) under GDPR, independent schools are not.

It is a requirement within GDPR that any organisation in control of processing personal data has to make certain information available through a Privacy Notice.

2. Objectives

This Policy aims to provide overarching guidance to all members of the RHS community concerning the application of data protection compliance. The objectives of data protection across RHS are summarised as follows:

- To enable the legitimate collection and recording of required personal data and information while avoiding the processing of unnecessary information.

- To record personal data accurately and keep it up to date.

- To use personal data for legitimate purposes only, and to ensure it is neither used nor distributed inappropriately.

- To ensure appropriate security processes are in place to protect personal data and prevent unauthorised access or usage.

- To ensure personal data is retained for only as long as is necessary, then properly disposed of.

- To ensure transparency in respect of individual rights, and to provide evidence of data protection legal compliance.

3. Key GDPR Terms

"Data" within GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria.

"**Personal Data**" includes everything from which a Data Subject can be identified. It ranges from simple contact details via the personnel department or pupil files to safeguarding information, and encompasses opinions, file notes or minutes, a record of anyone's intentions towards another person, and communications (such as emails) with or about them.

Some categories of Personal Data are "**special category data**" under the GDPR (broadly equivalent to "sensitive" personal data under the old law, but with criminal data treated separately). These comprise data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- health
- sex life or sexual orientation
- biometric data (new under GDPR – not currently applicable at RHS)

Extra safeguards are provided by law for the processing of such data[1]. Note that while not categorised as special category data, the processing of '**criminal offence data'** is also provided with extra safeguards[2].

"Data Controllers" means organisations, including RHS, that determine how people's personal data is processed and for what purpose. This places a requirement on RHS to have its own GDPR Policies and Privacy Notice.

[1] 'In order to lawfully process special category data you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9' – ICO Guide to GDPR.

[2] 'You must still have a lawful basis for your processing under Article 6, in exactly the same way as for any other personal data. The difference is that if you are processing personal criminal offence data, you will also need to comply with Article 10'. – ICO Guide to GDPR

"**Data Subjects**" means any living individuals whose data the Data Controller processes.

One of GDPR's core tenets is **"transparency"**, meaning an emphasis on data controllers telling data subjects how they use their personal data in clear language. This is to be provided to data subjects through an appropriate **"Privacy Notice"**.

"**Processing**" means any action in relation to that personal data, including filing and communication.

"Lawful Bases for Processing". Under GDPR Article 6, one of the following 6 categories must apply when processing personal data:

- Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract you have with the individual.
- Legal Obligation: the processing is necessary for you to comply with the law.
- Vital Interests: the processing is necessary to protect someone's life.
- Public Task: the processing is necessary for you to perform a task in the public interest
- Legitimate Interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is good reason to protect the individual's personal data which overrides those legitimate interests. (Does not apply to public authorities).

The most flexible lawful basis for processing people's data is **"legitimate interests"**, where their data is used in ways they would reasonably expect and which have a minimal privacy impact, or where there is compelling justification for the processing. Use of legitimate interest as a legal basis for processing data should only be permitted following a **"legitimate interest assessment (LIA)"**, which should be recorded to demonstrate compliance if required. Such an assessment should:

- Identify the legitimate interest.
- Show that the processing is necessary to achieve it.
- Balance it against the individual's interests, rights and freedoms.

'Consent'', when required, means offering individuals real choice and control. It requires a positive opt-in, not pre-ticked boxes or any other method of default consent.

"Children" have the same rights as adults over their personal data and are provided with additional protection under GDPR. A specific privacy notice and data protection education is provided for RHS pupils, and a separate policy applies to the taking, storage and use of pupil images.

If consent is required, only children aged 13 (or such other age as advised by the ICO) and above are able to provide their own consent; if under 13 (or such other age as advised by the ICO), consent is required from whoever holds parental responsibility.

Individuals have the right to **"access''** their personal data and supplementary information through subject access requests. The right of access allows individuals to be aware of and verify the lawfulness of the processing - an effective "**Privacy Notice"** should aim to cover this by explaining to all data subjects what personal data the School lawfully processes.

4. Application of Data protection and GDPR at RHS, and the Delivery of Compliance.

RHS is a Data Controller. In addition, RHS Charitable Trust (RHSCT) and RHS Enterprises Ltd (RHSEL) are also designated as separate Data Controllers for data processed in those entities. Data Controllers are required to ensure that any personal data processed on their behalf is done so in compliance with the requirements of GDPR; to this end both RHSCT and RHSEL are to observe the overarching School policies in relation to Data Protection as well as maintain their own Privacy Notices and LIAs. RHSCT and RHSEL will maintain separate registrations with the ICO.

As far as the School is concerned, the overarching legal basis for processing data under GDPR has been identified and recorded within an LIA as 'legitimate interest', with additional conditions identified and applied in respect of:

- Special category data (pupil health information) – Article 9(2) (a).
- Special category data (trade union membership) – Article 9 (2) (b).
- Special category data (staff occupational health) – Article 9(2) (h).
- Special category data (racial or ethnic origin) – Article 9(2) (j).
- Criminal offence data (DBS checks) – Article 10.
- Images of pupils – consent where required according to the Taking, Storage and Using Images of Children Policy

The overarching School Privacy Notice is available at www.royalhospitalschool.org and aims to explain to all data subjects why and how personal data is controlled and processed across the RHS community, past and present.

In addition to this overall Notice, separate more focused Privacy Notices are provided for:

- RHS Charitable Trust/Alumni
- RHS Enterprises Ltd
- Pupils
- Contractors
- Staff and new staff applicants
- Music At RHS
- RHS website

5. Responsibilities.

All Staff Awareness. All staff at RHS are to have an appropriate level of awareness of and training in the management of data protection and GDPR commensurate with their individual roles and any responsibilities for data control/processing[3]. There is the constant need for all staff to minimise the processing of personal data, and to ensure that such data is always correctly handled. Retention of personal data and emails is to be minimised.[4]

Parent and Pupil Awareness. The Director of Communications is responsible for the Taking, Storage and Using Images of Children Policy, and for ensuring parental awareness of RHS data protection processes

[3] On-Line training for GDPR Essentials and GDPR Management is provided through IHASCO.
[4] In accordance with the School's Data Documentation, Information Security and Retention Policy.

through the website and the pupil application and parent contract processes. The Head of Digital Strategy is responsible for the delivery of pupil data protection procedures[5] and education.

Privacy and Compliance Officer. The Director of Finance and Operations (Bursar) is the designated RHS Privacy and Compliance Officer. He has overall responsibility for the School's execution of data control and the delivery and maintenance of data protection and GDPR compliance, including awareness/training, periodic data processing audits, access and retention checks, and the handling of subject access requests and personal data breaches.

School Departments. All Heads of Department are responsible to the Privacy and Compliance Officer for delivery and maintenance of GDPR compliance within their Department. This includes the management of any 3rd Party personal data processing arrangements contracted by their Department.

Information Systems Manager. Responsible for providing IS enablers and security to support legal and legitimate data processing, and for meeting subject access requests. Also responsible, where necessary for Safeguarding, for monitoring of emails, internet and telephone usage within GDPR guidelines. Lead on Data Protection Impact Assessments (DPIAs) and Data Protection by design in relation to any new processes and technology. Supervision of Data Manager and iSAMS processes.

6. Documentation.

GDPR places additional documentation obligations on organisations such as RHS with over 250 employees that control and process data. This includes maintaining a record of processing activities plus data sharing and retention. The responsibility for these additional obligations rests with the Privacy and Compliance Officer[6].

7. Personal Data Breaches.

GDPR introduces a duty on all organisations to report certain types of personal data breaches to the ICO within 72 hours. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. Examples of personal data breaches include:

- Access by an unauthorised third party
- Deliberate or accidental action by a data processor or controller
- Sending personal data to the incorrect recipient
- Sharing personal data via social media
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Any personal data breach that is identified within the RHS community is to be contained as swiftly as possible and reported immediately to the Privacy and Compliance Officer, who will assess if a report to the ICO is required based on the risk to 'people's rights and freedoms'.

[5] Pupil Digital Handbook, Pupil Privacy Notice, On Line Safety Policy etc.
[6] Key author of the Data Documentation, Information Security and Retention Policy.

In the event of any 'outsourced' processing of RHS personal data being breached, it must be reported to the Privacy and Compliance Officer as quickly as possible and if assessed as necessary a report is to be forwarded by him to the ICO.

A breach notification to the ICO is to include the following information:

- Description of the nature of the personal data breach including where possible
    - Categories and approximate number individuals concerned
    - Categories and approximate number of personal data records concerned
- Contact details of the Privacy and Compliance Officer
- Description of the likely consequences of the personal data breach
- Description of measures taken/planned to deal with and mitigate the breach