RUGBY SCHOOL GROUP

Data Protection Policy

April 2024

1. INTRODUCTION

1.1 The Rugby School Group (the 'Group') is required to process personal data regarding staff, students and their parents and guardians and friends of the Group relevant to its operation and shall take all reasonable steps to do so in accordance with this Policy. In this Policy any reference to students, parents, friends or staff includes current, past or prospective students, parents, friends or staff.

1.2 All staff are responsible for complying with this policy, (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, governors, contractors, agency staff, work experience / placement, students and volunteers.

2. SCOPE

2.1 This Policy covers Group's acquisition, processing and disposal of the personal and sensitive personal data it holds on all staff, including temporary staff, agency workers, volunteers, parents, students and other third parties. It also applies to Governors and contractors. It explains the Group's general approach to data protection which is to ensure that an individual's personal data and information is protected and appropriately processed and provides practical guidance which will help to ensure that the Group complies with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

2.2 Rugby School Group in this policy refers to the main Charity, 'Governing Body of Rugby School', including Rugby School, Bilton Grange, and all its legal subsidiaries, either individually or collectively. For the avoidance of doubt the scope of this policy does not include the Group's international schools (currently Rugby School Thailand and Rugby School Japan).

2.3 All staff, governors and directors who handle the personal data of students, parents and staff should read and familiarise themselves with this policy. It should form part of the suite of policies signed off by new staff, governors and directors.

3. DEFINITIONS

3.1 Personal data is:

- any information about a living person who can be identified (e.g. their name, address, online identifier such as an IP address, academics, school activities, attendance record, discipline, bank details and/or financial information in relations to parents and/or guardians, special education needs, exam results, images of students engaging in school activities, references or expressions of opinion about them). It makes no difference if they can be identified directly from the record itself or indirectly using other information in the Group's possession or likely to come into the Group's possession.
- Personal information that has been, or will be, word processed or stored electronically (e.g. computer databases and CCTV recordings), personal information that is, or will be, kept in a file (either physical or digital) which relates to an individual or in a filing system that is organised by reference to criteria which relate to the individuals concerned (e.g. name, school year, school activities).

- Sensitive personal data is any information about a person's race, ethnic background, political opinions, religious beliefs, trade union membership, genetics, biometrics (where used for identification), health, sex life or orientation, criminal offences or alleged offences and any proceedings.

3.2 The Group has additional obligations in connection with the use of sensitive personal data. At least one of the following conditions or those others outlined in Article 9 of the UK GDPR must be satisfied in order for the data to be retained and used. Please contact the Information Security Officer if you have questions relating to this.

- Explicit consent of the data subject must be obtained
- Necessary for carrying out the obligations under employment, social security or social protection law or a collective agreement
- Used in connection with alumni relations provided it relates solely to this and there is no disclosure to a third party without consent
- Data manifestly made public by the data subject
- Various public interest situations as outlined in the GDPR and the Data Protection Act 2018

3.3 The data subject is:

The person the information relates to. There may be more than one data subject, such as when a record concerns an incident involving two students.

3.4 The Data Controller:

The Group is the Data Controller and is responsible for determining the purposes of its use of data - what data it gathers and how this information is used. As the Data Controller the Group is responsible for complying with the GDPR.

3.5 Data Processor:

An organisation that processes personal data on behalf of a controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.

3.6 Processing:

This covers virtually anything done with personal data, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

3.7 The Information Security Officer:

The Group has appointed the Operations Director as its Information Security Officer, responsible for day to day compliance with this Policy. They can be contacted at The Bursary, 10 little Church Street, Rugby, CV21 3AW or at infosecurity@rugbyschool.net.

4. PRINCIPLES

4.1 The UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by controllers (and processors). These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;

4. **Accurate** and kept **up to date**;

5. **Kept for no longer than is necessary** for the purposes for which it is processed; and

6. Processed in a manner that ensures **appropriate security** of the personal data.

4.2 The UK GDPR's broader 'accountability' principle also requires that the Group not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments ("DPIA")); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

5. ACQUIRING, USING AND DISPOSAL OF PERSONAL DATA

5.1 The Group shall only process personal data for specific and legitimate interests including:

- providing students and staff with a safe and secure environment including images on CCTV – all cameras around the Group carry appropriate warning signs as to their operation. They are used for the purpose of detecting crime, ensuring personal security and the welfare of staff and students and the protection of the working environment. Images are kept no longer than 28 days to meet these objectives. However, in certain circumstances (such as an on-going investigation into criminal activity) certain relevant images may be kept for longer, but no longer than necessary to complete any such investigation.
- providing education, training and pastoral care.
- providing activities for students and parents - this includes school trips and activity clubs.
- providing academic, examination and career references for students and staff.
- protecting and promoting the interests and objectives of the Group - this includes fundraising and commercial ventures.
- safeguarding, child protection and promoting the welfare of students.
- monitoring student and staff email communications, internet and telephone use to ensure students and staff are following the Group's Online Safey Policy including Staff (and Volunteer) Acceptable Use policy.
- promoting the Group to prospective students and their parents.
- communicating with former students of all schools in the wider Rugby School Group, including those overseas.
- for personnel, administrative and management purposes. For example, to pay staff and to monitor their performance.
- fulfilling the Group's contractual and other legal obligations.

- for the administration of enquiries and applications for admission to the Group including details of parents/guardians and children.
- processing bills and collecting payments.

5.2 Staff should seek advice from the Information Security Officer before using personal data for a purpose which is different from that for which it was originally acquired. If information has been obtained for one purpose, it shall not be used for any other purpose without the Information Security Officer's permission.

5.3 The Group shall not hold unnecessary personal data, but shall hold sufficient information for the purpose for which it is required. The Group shall record that information accurately and shall take reasonable steps to keep it up-to-date. This includes an individual's contact and medical details.

5.4 The Group shall not transfer personal data outside the European Economic Area (EEA) without the data subject's permission unless it is satisfied that the data subject's rights under the GDPR will be adequately protected and the transfer has been approved by the Information Security Officer. This applies even if the transfer is to a student's parents or guardians living outside the EEA**.**

5.5 When the Group acquires personal information that will be kept as personal data, the Group shall be fair to the data subject and fair to whoever provides the information (if that is someone else) in that their data will be handled and safeguarded in compliance with the GDPR.

5.6 The Group shall only keep personal data for as long as is reasonably necessary and in accordance with the retention and disposal guidelines set out in the Group's Document Retention Policy. Staff should not delete records containing personal data without authorisation.

5.7 The Group will keep personal data secure and adopt technical and organisational measures to prevent unauthorised or unlawful processing of personal data.

6. INFORMATION AND EXPLANATION

6.1 Privacy Notice: Individuals must be told what data is collected about them, and what it is used for. This is called a privacy notice or statement.

6.2 Purpose: The privacy notice is to ensure that the Group's collection and processing of personal data is done in a transparent way so it will explain who it applies to, why the information is being collected, what information will be collected, how it will be acquired and processed, what it will be used for, which third parties (if any) it will be shared with and outline the data subject's rights, including the right to complain about the processing of their data to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow. Cheshire SK9 5AF, telephone 0303 123 1113 or at: https://ico.org.uk/concerns/.

6.3 Staff are not expected to routinely provide students, parents and others with a privacy notice as this should have already been provided. Copies of the Group's privacy notices for students and parents can be obtained from the Information Security Officer or accessed on the Group's websites.

6.4 Use: Having said this, staff should inform the Information Security Officer if they suspect that the Group is using personal data in a way which might not be covered by an existing privacy notice. This may be the case where, for example, staff are aware that the Group is collecting information about students without telling their parents what that information will be used for.

7. PROTECTING CONFIDENTIALITY

7.1 Disclosing personal data within the Group: Personal data should only be shared on a need to know basis. Personal data shall not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority within the Group or their relationship to the data subject, unless they need to know it for a legitimate purpose. Examples include:

- the School Nurse may disclose details of a cleaning lady's allergy to bee stings to colleagues so that they will know how to respond, but more private health matters must be kept confidential.
- Personal contact details for a member of staff (e.g. their home address and telephone number, and their private mobile telephone number and e-mail address) shall not be disclosed to parents, students or other members of staff unless the member of staff has given their permission.

7.2 Disclosing personal data outside of the Group: Sharing personal data with others is often permissible so long as doing so is fair and lawful under the GDPR. However, staff should always speak to the Information Security Officer if in doubt, or if staff are being asked to share personal data in a new way.

7.3 Before sharing personal data outside the Group, particularly in response to telephone requests for personal data staff should:

- make sure they are allowed to share it – that they have the necessary consent;
- ensure adequate security. What is adequate will depend on the nature of the data. For example, if the Group is sending a child protection report to social services on a memory stick then the memory stick must be encrypted; paper information should be sent by courier or special delivery, First or Second Class post is not considered secure enough and
- make sure that the sharing is covered in the privacy notice.

7.4 The Group should be careful when using photographs, videos or other media as this is covered by the GDPR as well. Specific guidance on this is provided in the Group's Images Policy available on the Group's websites.

7.5 Information security and protecting personal data: Information security is the most important aspect of data protection compliance and most of the fines under the GDPR for non-compliance relate to security breaches. The Group shall do all that is reasonable to ensure that personal data is not lost or damaged, or accessed or used without proper authority, and the Group shall take appropriate steps to prevent these events happening. In particular:

- paper records which include confidential information shall be kept in a cabinet or office which is kept locked when unattended.
- the Group uses a range of measures to protect personal data stored on computers, including file encryption, anti-virus and security software, sufficiently robust and frequently changed user passwords, audit trails and back-up systems.
- staff must not remove personal data from the Group's premises unless it is stored in an encrypted form on a password protected computer or memory device. Further information is available from the Director of IT.
- staff must not use or leave computers, memory devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons: they should not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased.

- Personal data exchanged internally via email must be limited to that which is absolutely necessary.

7.6 Use of third party platforms / suppliers. As noted above, where a third party is processing personal data on the Group's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a DPIA before proceeding – particularly if the platform or software involves any sort of novel or high risk form of processing (including any use of artificial intelligence ("AI") technology). Any request to engage a third party supplier should be referred to the Information Security Officer in the first instance, and at as early a stage as possible.

8. DATA BREACHES

8.1 Definition: A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

8.2 Reporting obligations: Any actual data breach or alleged data breach must be reported to the Information Security Officer as soon as it is discovered to enable its circumstances to be investigated and appropriate action taken to limit any damage and to prevent a similar occurrence. As soon as the Group becomes aware of a significant data breach as determined by the Information Security Officer it has 72 hours in which to report the breach to the Information Commissioner's Office. Examples of breaches and their seriousness for reporting purposes are:

- mistakenly sending an email containing personal data to an incorrect recipient.
- theft of IT equipment containing personal data.
- failing to deal with a Subject Access Request.

If a breach is found to be sufficiently serious i.e. if not dealt with it is likely to result in a high risk to the rights and freedoms of individuals e.g. resulting in discrimination, damage to reputation, financial loss – through identity theft or otherwise – loss of confidentiality or any other significant economic or social disadvantage then not only does this breach have to be reported to the ICO within 72 hours of its discovery, the individuals concerned must be notified of the breach in a timely manner as directed by the Information Security Officer.

9. DATA SUBJECT'S RIGHTS, INCLUDING ACCESSING ANY DATA HELD ON THEM

9.1 Individuals are entitled to know whether the Group is holding any personal data which relates to them. This is known as a Subject Access Request.

9.2 Any member of staff wishing to exercise the right to access information covered by this policy, can do so by submitting an access request verbally, in writing or by email to the Information Security Officer.

9.3 Any member of staff who receives a request to access information covered by this policy from a student, parent or any other individual must inform the Information Security Officer as soon as is reasonably possible, normally on the same day. This is important as there is a statutory procedure and timetable which the Group must follow. The Group has only one month to respond to a Subject Access Request from whenever the request is received.

9.4 Individuals have a right to ask the Group not to use their personal data for direct marketing purposes or in ways which are likely to cause substantial damage or distress.

9.5 Individuals have a right to ask for incorrect personal data to be corrected or annotated.

9.6 Individuals have the right to object to any of their personal data being processed and to have this data erased.

9.7 Individuals have the right to restrict (halt) the processing of their personal data, usually whilst incorrect data is being corrected.

9.8 Individuals have the right to request their personal data is transferred to another data controller in a commonly used electronic format.

9.9 Individuals have a right to ask the Group not to make automated decisions (using personal data) if such automated decisions using pre-programmed software would affect them to a significant degree.

9.10 Individuals have the right to complain about the processing of their personal data to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, Telephone 0303 123 1113 or at: https://ico.org.uk/concerns/.

9.11 A person may be committing a criminal offence if they alter, block, erase, destroy or conceal information to prevent it from being disclosed (for example, to prevent its disclosure under a subject access request). Therefore, if you are asked to provide information or documents to a colleague who is preparing a response to a subject access request then you must make sure that you provide everything.

10 PROCESSING OF FINANCIAL / CREDIT CARD DATA

10.1 The Group complies with the requirements of the PCI Data Security Standard ("PCI DSS"). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the Finance Director. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

11. FURTHER INFORMATION

11.1 The Group has registered its use of personal data with the Information Commissioner's Office and further details of the personal data it holds, and how it is used, can be found in the Group's register entry on the Information Commissioner's website at www.ico.gov.uk under registration number Z6175287. This website also contains further information about data protection.

12. BREACH OF THIS POLICY

12.1 Any breach of this policy may result in disciplinary action.

12.2 A member of staff who deliberately or recklessly accesses or discloses personal data held by the Group without proper authority, or without a business need to do so maybe guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

13. STATUS

13.1 This policy is intended only as a statement of Group policy. It does not form part of the contract of employment and may be amended from time to time.

14. POLICY OWNER

14.1 The owner of this policy is the Information Security Officer.

15. RELATED POLICIES

- Staff Discipline Policy
- Online Safety Policy including Staff (and Volunteer) Acceptable Use Policy
- Communications Policy
- Privacy Notice for Staff
- Privacy Notice for Parents and Guardians
- Privacy Notices for Students
- Privacy Notice for Users of Rugby School Sports Centre
- Document Retention Policy
- Images Policy

16. FURTHER INFORMATION

16.1 Further information and guidance regarding this policy or its application can be obtained from the Information Security Officer – infosecurity@rugbyschool.net

Authorised by the Risk, Compliance & Safeguarding Committee	**May 2024**