GDPR-DATA PROTECTION POLICY



GDPR DATA PROTECTION POLICY

Newcastle upon Tyne Royal Grammar School

The **UK GDPR** and the **UK Data Protection Act 2018** (*the Acts*) replaced the Data Protection Act 1998 on 25 May 2018. The fundamentals remain the same but there are significant changes. (note: Although the UK has now left the EU and is no longer subject to EU law, it has passed a version of the GDPR into UK law (the 'UK GDPR'), to sit alongside the UK Data Protection Act 2018 ('DPA 2018').

This policy is updated to reflect the Data (Use and Access) Act 2025, which amends elements of the UK GDPR and Data Protection Act 2018 relevant to schools, including subject access requests, complaints handling, automated decision-making, children's privacy protections, and recognised legitimate interests.

The school has published a PRIVACY NOTICE that details how the school will use (or "process") personal data about individuals. This includes both staff information, but also how staff should handle other staff, students, parents and alumni information.

WHO DOES THIS POLICY APPLY TO?

This Policy is primarily aimed at staff: it describes how, as a matter of good practice and policy, any personal data controlled and processed by the RGS Group of Schools – including parents, pupils, contractors and colleagues (past, present or prospective) – should be handled in accordance with law and best practice. Where such staff are concerned, this Policy will inevitably therefore have some overlap or interaction with other policies concerning how staff handle data, notably IDT: Acceptable Use, Social Media/Use of Images, Retention of Records, and Safeguarding (including record keeping and information sharing).

For the purposes of this notice, the RGS Group comprises of:

- The Royal Grammar School, Newcastle upon Tyne ("RGS Newcastle")
- Westfield School
- Any subsidiary company, charitable entity, trading company or associated organisation operating under the governance or control of the RGS Group from time to time.

References throughout this Privacy Notice to "the School", "the School's", "the RGS Group", "we", "our" or "us" mean the relevant member institution within the RGS Group that is collecting or processing personal data, or the RGS Group collectively where activities are carried out on a shared basis.

TO WHAT INFORMATION DOES IT APPLY?

Like the Data Protection Act, the UK GDPR only applies to 'personal data' and 'special personal data'.

DEFINITIONS

Key data protection terms used in this data protection policy are:

- Data controller – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including by its [trustees/directors/governors]) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.

- Data processor – an organisation that processes personal data on behalf of a data 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.

- Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- Personal information (or 'personal data'): any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes

expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.

- Processing – virtually anything done with personal information, 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.

- Special categories of personal data – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

PERSON RESPONSIBLE FOR DATA PROTECTION IN SCHOOL

The School has appointed the Director of Finance & Operations as the Data Protection Officer who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of applicable data protection legislation. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer.

THE SEVEN PRINCIPLES OF DATA PROTECTION

The seven principles that users of data need to adhere to are that data is:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;

- collected for specified, explicit and legitimate purposes;

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

- accurate and, where necessary, kept up to date;

- 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;

- 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; and

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

LAWFUL GROUNDS FOR DATA PROCESSING

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests' and in order to carry out its ordinary duties to staff, students and parents, the school needs to process a wide range of personal data about as part of its daily operations. For the vast majority of the information we hold there is therefore a legitimate interest or legal requirement for us to hold it and consent from the individual is not required.

The School's legitimate interests are set out in its Privacy Notice, as GDPR requires.
Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;

- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;

a narrower set of grounds for processing breachgories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

WHEN SHOULD CONSENT BE SOUGHT?

Consent needs to be sought when one of the other legitimate processing criteria cannot be applied. For when consent is required verbal consent, or consent by action, could work legally. However, one of the core requirements in GDPR is for careful and provable record-keeping – so written consent should be sought.

The aspects for which we need consent are: use of photographs and images (unless specified within the Parent Contract); university applications; for overseas visits where personal details are being sent to an overseas third party, for example for visa applications; and applications to overseas universities. If you have a doubt about whether consent is required, ask.

CHILDRENS GDPR RIGHTS

Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

Third party technology platforms used by students are assessed to ensure that data collection is minimised and that high privacy settings are enabled, unless it is demonstrably in the best interests of the child and their education.

The school does not enable geolocation features for pupils unless strictly necessary for the delivery of a specific educational activity.

RESPONSIBILITIES OF ALL STAFF

1. Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that any personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests***. However, the starting position for staff is to record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it.***

2. Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with the *Staff Code* and all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:
Safeguarding & Child Protection Policy; Privacy Notice; Record Retention Procedure & Schedule; IT Acceptable Use Policy; Taking, Storing and Using Images Policies; and the Staff Code (including references within it to the use of social media and remote working).

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

3. Avoiding, mitigating and reporting data breaches

One of the key obligations contained in the UK GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals)

to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach, they must notify the Director of Finance & Operations. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

4. Care and data security

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles, and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that affects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to the Director of Finance & Operations, and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

STORAGE AND ACCESS TO DATA

Data stored on school servers and the network, such as personal drives and shared drives (Microsoft365) and in applications such as iSAMS, SAGE, HR Pro, iFinance, Evolve is secure and should not cause any issues when accessed from devices attached to the school network within the school. Accessing the school systems from outside the school should be done using Multi Factor Authentication. However, staff should not download school personal files to personal devices as outlined in the ACCEPTABLE USE POLICY.

MAINTAINING, RETENTION AND DESTRUCTION OF DATA

The RECORD RETENTION PROCEDURE AND SCHEDULE gives guidance on storing, retaining and if necessary, destroying data. The procedure identifies data holders, but it is the responsibility of all staff to ensure that personal information is managed properly. This is essential to being able to demonstrate compliance with the principles.

Destruction of data needs to be recorded and so if staff feel that any data is no longer required they should consult with the identified data holder in the first instance and if required a member of the SLT.

USE OF THIRD-PARTY SOFTWARE AND APPS

There are many apps and software that are useful and can be used without any GDPR issues. Examples are online exercises and revision tutorials. The key consideration is whether personal data is being uploaded to the application. For the majority of applications which are accessed by just a log in name and password that is supplied by the student there is no GDPR requirement.

For applications that require personal data then confirmation is required that the organisation is complying with the GDPR requirements. IDT Services will complete an assessment of all third-party software and applications for compliance. A record of this confirmation must be passed to the Director of Finance and Operations (DFO) before the application is used.

For technology used by students, there will be a consideration of the children's needs and comply with DUAA (2025) privacy-by-design obligations.

RIGHTS OF INDIVIDUALS / SUBJECT ACCESS REQUESTS

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School). This is known as the **'subject access right**' (or the right to make **'subject access requests'**).

Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you should note the date the request is received and should inform the DFO immediately. The circumstances of the request will determine what action needs to be taken. In any event the school has to respond within one month. The DUAA (2025) allows the School to pause the response time, without the risk of missing the deadline, if data subjects need to clarify or refine their requests or to provide more information. Any requests and searches specifically need to be reasonable and proportionate.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller; and
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the DFO as soon as possible.

DATA PROTECTION COMPLAINTS PROCEDURE

- Under the Data Usage and Access Act (2025) School's must now provide clear routes for data protection complaints. Any complaints will be acknowledged within 30 days. Responses are the responsibility of the DFO. Any data protection complaints should be made in writing to the DFO at dataprotection@rgs.newcastle.sch.uk

AUTOMATED DECISION-MAKING AND USE OF AI

The School does not currently use artificial intelligence (AI), profiling, or solely automated decision-making processes to make decisions about pupils, parents, carers, staff, governors, volunteers or visitors.
Any decisions that may affect an individual are made by appropriately authorised members of staff and include meaningful human review and oversight.
Should the School introduce AI-enabled systems or automated decision-making technologies in the future that process personal data, the School will:

- undertake appropriate data protection and privacy impact assessments;
- ensure compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and relevant Department for Education guidance;

- assess the necessity, proportionality, fairness and transparency of any processing;
- implement appropriate safeguards to protect the rights and freedoms of individuals;
- provide clear privacy information explaining how personal data is being processed; and
- ensure that individuals are able to exercise any rights available to them under data protection legislation.

The School recognises the growing use of AI technologies and will continue to monitor guidance issued by the Information Commissioner's Office (ICO), the Department for Education (DfE) and other relevant regulators to ensure that any future use of such technologies remains lawful, fair and transparent.

DATA MINIMISATION AND AUDIT

- The school operates a strict Data Minimisation and Audit process, carrying out quarterly reviews of the data held, maintaining clear documentation that justifies each category of personal data collected, and ensuring that any information no longer required for a lawful purpose is securely deleted in line with ICO expectations on minimisation and retention.

PRIVACY BY DESIGN

When considering the introduction of a new procedure, process or new software, GDPR requires that consideration and inclusion of appropriate data protection is made during the design phase of all new projects and changes to systems and processes. Further guidance can be obtained from DFO.

SUMMARY

It is in everyone's interest to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

MORE INFORMATION

For more information see PRIVACY NOTICE and RECORDS RETENTION POLICY in the Staff Handbook.

ANY QUERIES?

If you have any queries about GDPR then please contact the DFO at dataprotection@rgs.newcastle.sch.uk

CONTACT DETAILS

Royal Grammar School, Eskdale Terrace, Newcastle upon Tyne NE2 4DX

Tel: 0191 281 5711

General enquiries: communications@rgs.newcastle.sch.uk

www.rgs.newcastle.sch.uk