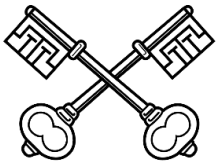

RADLEY

Data Processing Procedures

January 2024

Data Processing Procedures

Data Processing Procedures

This is an internal document detailing how members of staff at Radley College should manage data. It should be read in conjunction with the public facing Privacy Statement and the Fundraising Policy.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) (adopted 2016), has been enforceable since 25 May 2018 and replaced previous legislation such as the Data Protection Act (DPA 1998).

- The GDPR broadens the DPA's scope of personal data by including more detailed personal identifiers (e.g IP, MAC addresses, cookies etc).
- The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria.
- The UK Information Commissioners' Office ("ICO") can currently issue fines of up to £8.7m for a UK organisation that seriously breaches the DPA. For major breaches the GDPR raises fines up to €20m, or 4% of annual global turnover (whichever is higher).
- The GDPR introduces an accountability principle which requires organisations to demonstrate compliance through a series of actions.
- The GDPR strengthens the rights of individuals:
    - Right to be informed (concise, clear and free);
    - Right of access (faster response times for SARs/free);
    - Right of rectification (faster response times/3rd parties);
    - Right to erasure (faster response times/3rd parties);
    - Right to restrict processing;
    - Right to data portability (automated processing only);
    - Right to object; and
    - Rights to automated decision making and profiling

Significant changes from DPA

- The GPDR places special legal obligations on data processors to maintain records of personal data and processing activities.
- Whereas the DPA did not require organisations to report data breaches, GPDR mandates they "notify the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it".
- Data subjects (employees and customers) now have the power to request the deletion or removal of their personal data, including back-ups, archived data and from 3rd parties (eg cloud or storage).
- Individuals now have the right to initiate data portability requests to obtain their personal data and reuse it as they wish. Organisations are obliged to comply.

- There are now new provisions to protect children's personal data. Privacy notices will need to be written in clear, understandable language and where services are targeted at children, consent from a parent or guardian will also be required.
- Organisations need to incorporate GDPR requirements in data collection processes and consider use of new technology to ensure "privacy by design" including through data minimisation and pseudonymisation.

Radley and the GDPR

Radley strives to follow the principles outlined above. The school has chosen not to appoint a Data Protection Officer, data protection queries should be referred to the Bursar.

There are a number of designated data controllers covering the following areas:

- Current pupils and parents core data
- Pastoral data
- Academic data
- Co-Curricular data
- Medical data
- Prospective pupils and parents
- Former pupils and parents
- Prospective, current and former staff
- Sports Centre
- Lettings
- Choristers

Data Security

The GDPR is concerned with personal data handled by organisations in both electronic and physical formats, such as paper documents.

All personal data, whether in hard copy or stored on a USB, CD, or other physical device must be kept in a secure environment with controlled access. Appropriate secure environments include:

- Locked metal cabinets with access to keys limited to staff only
- Locked drawer in a desk (or other storage area) with access to keys limited to staff only
- Locked room accessed by key or coded door lock where access to keys and/or codes is limited to authorised staff only

Files containing personal data must never be left unattended while removed from their normal locked storage area. Staff should therefore adopt a clear desk policy, in relation to files and documents containing personal information, at all times when they are out of their offices or away from their work area.

Any machine connected to the Radley College network has the potential to give access to a large amount of personal data.

- Unattended machines and devices must be locked or logged out. This is especially important for machines in unlocked public spaces such as classrooms. To immediately lock your

computer, press the windows button and the letter L key, or press Ctrl-Alt-Del, and then click Lock this computer, Lock Computer, or Lock. All personal devices must have suitable security enabled (passwords / fingerprint recognition etc).
- Passwords should be changed regularly. Help and instructions can be found at https://radley.fireflycloud.net/it-help/passwords.

The above will form part of the induction and ongoing training of staff. Breaches will be taken very seriously.

Staff are strongly encouraged to store data in the cloud (Office 365 or similar). This adds security and allows the user to access the data from different devices.

Data Encryption

Data of a Private, Sensitive or Confidential nature should be Encrypted both at rest (when stored) and in transit (when sent). In practice this means that:

- Devices should be securely "Locked" either physically or digitally when they are not being used. Strong passwords or biometrics must be used. Dual-factor should be employed wherever practical.
- Auto screen locks should be used. Be wary of allowing "Notifications" to break through screen locks.
- Encryption should be enabled. If in doubt, ask how this is done.
- Data should be "shared" on a suitably secure cloud platform (eg Office 365, MIS) rather than sent as an attachment.
- Data-sticks, SD cards and other such mobile storage devices should NOT be used either to store or transfer any data of a private, sensitive or confidential nature

These requirements apply to all computing devices including Desktop PCs. Laptops, tablets, phones and other mobile devices are particularly vulnerable and users should take particular care when using such devices.

Data Breaches

Where a data breach is known to have occurred (or is suspected) any member of staff who becomes aware of this must alert the IT Department in the first instance.

The information that should be provided (if known) includes:

- When the breach occurred (time and date)
- Description of the breach (type of personal information involved)
- Cause of the breach (if known) otherwise how it was discovered
- Which system(s) if any are affected?
- Who is involved?
- Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach)

Legal Basis for Data Processing

For processing to be lawful under the GDPR, the school needs to identify a lawful basis before it can process personal data. It is important that we determine the lawful basis for processing personal data and document this in our Privacy Statement.

There are six available lawful bases for processing:

- Consent. The data subject has given consent to the processing. Please note that rules around consent are much stricter under GDPR. Consent means offering individuals genuine choice and control and requires a positive opt-in. Pre-ticked boxes and any other methods of consent by default are not lawful.
- Contract. Processing is necessary for the performance of a contract with the data subject
- Legal Obligation. Processing is necessary for compliance with a legal obligation
- Vital Interests. Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Public Task. Processing is necessary for the performance of a task carried out in the public interest
- Legitimate Interests. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

The school's lawful basis for processing personal data is legitimate interests, unless otherwise stated.

Address Lists

In general, contact details are best stored in the School Database.

However there will be occasions when it is pragmatic to keep separate lists of contact details. Examples include:

- The Choral Society (a mixture of staff, partners, parents, and friends of Radley)
- The Sewell Gallery invitation list

In these cases it is acceptable for the data to be stored in other ways such as a spreadsheet but care must be taken to ensure that the data is:

- **Accurate** (up to date and not including anyone who does not wish to be contacted) and
- **Secure** (eg stored on OneDrive and password protected).

Sharing contact details / email addresses

Parental contact details are sensitive data. Some parents are very happy for these to be shared within the parental body and with selected outside companies but others are more protective of them. We need to respect these views. GDPR means that we need to be more careful about obtaining explicit permission for data to be shared.

1. Sharing the contact details within the parent body.
    - Parents are often keen to get in touch with parents of other boys (usually within a year group in a Social).

- Before sharing these details a Tutor must obtain (and retain) written permission (by email is fine) from each parent in which it is clear:
    - what is being shared (email / address / telephone number etc).
    - how long the permission remains valid for (e.g. the duration of the boy's time at Radley).

2. Parents and other groups wanting to contact other parents for a specific purpose
    - If we feel that the email is reasonable then we can help facilitate communications such as:
        - organising a social gathering,
        - making arrangements for meeting at a sporting event (e.g. the Mariners),
        - initiating a collection for a leaving present (but see also the anti-bribery policy),
        - informing parents about opportunities organised by external companies such as foreign exchange visits, ordering photographs or mouthguards etc.
    - The person initiating the communication should write an email which includes their address for replies.
    - This should be vetted by the relevant member of staff at Radley and a member of SMT.
    - The email is then sent from Radley. Whether the recipients reply (and hence reveal their email address) is their decision.
    - The same principles apply to sharing contact details for other groups (boys, ORs, OR parents etc).

3. In some cases it may be necessary to share data with third parties such as mailing houses or software companies (eg Office 365, SchoolBase, Firefly, SOCS, Raisers Edge, Oasis, Earnie, Oliver, NHS, Westminster, Active Directory).

In such cases the relevant data controller must request a copy of the company's privacy policy and establish that the data will be kept securely and for the intended purpose only and that it will be deleted once used.

The data controller can use the Data Processing Agreement template.

Websites and intranet

The DDA is concerned to ensure that public websites are designed to maximise access to the web for all, regardless of disability. The school website is being designed to incorporate as many of the recommendations as are feasible.

So far, intranets are not included within the code of practice, however the Code of Practice for schools recommends that schools do not discriminate against disabled pupils and prospective pupils in the provision of education and associated services.

There is a section on the intranet (https://radley.fireflycloud.net/acsupp) which includes advice, computer programs and links for most DDA and Learning Support issues. Further information and access options examples from: www.equalityhumanrights.com.

Requests for Information

From time to time Old Radleians and others request information about their time at the school.

Care should be taken in:

- Deciding whether they are entitled to this information; and
- Establishing whether the person making the enquiry is who they say they are. For example before passing on sensitive information to an OR they should be asked to confirm their Social, matriculation year and date of birth.