ROYAL HIGH BATH

GDST
GIRLS' DAY SCHOOL TRUST

GDPR - DATA PROTECTION

Applicable to: All staff, governors, students and parents.

Objective

To provide our students with a first class education we collect and use the personal information of staff, pupils, parents and other individuals, who are referred to within this policy as 'data subjects'. The aim of this policy is to protect the fundamental rights and freedoms of these data subjects.

Procedure

The *Data Protection Act 2018* controls how personal information is used by organisations, and is the UK's implementation of the General Data Protection Regulation (GDPR). All staff involved with the collection, processing and disclosure of personal information are individually responsible for adhering to data protection legislation, together with the procedures outlined in this policy.

'**Personal data'**

This means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual;

Data protection principles

All staff using personal data must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, up-to-date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

Special categories of personal data

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs

- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

Data subject rights

Under the Data Protection Act 2018, data subjects have the right to find out what information organisations store, collect and process about them.

This includes the right to:

- be informed about how their data is being used
- access their personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of their data
- data portability (allowing you to get and reuse your data for different services)
- object to how their data is processed in certain circumstances.

Data Protection Officer (DPO)

The role of DPO is defined by law, and GDPR states that; '*Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.*'

GDPR provides guidance on the role of a DPO.

It advises that the data protection officer has to:

1. inform and advise the data controller and the employees who carry out processing of their obligations
2. monitor compliance with the Regulation, including assigning of responsibilities, raising awareness and staff training
3. provide advice where requested as regards the data protection impact assessment
4. cooperate and act as the contact point for the Information Commissioner's Office (ICO)

Independent Regulatory Body

The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. Further information about the ICO can be found on The Hub.

Privacy notice

The GDST's privacy notice provides a summary of how and why we process personal information. A copy of this notice can be found on The Hub.

Procedures

The following sections provide further information on how the data protection principles should be applied.

Information access (also referred to as Subject Access Request - SAR)

Data subjects have rights to access to personal information held or processed by the GDST. Further information on how a data subject may access their personal data can be found via a link on The Hub.

Data breach

A 'personal data breach' is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Further information on the GDST data breach reporting procedure can be found via a link on The Hub.

Retention of personal information

Data must not be 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. Further information on our retention schedules can be found via a link on The Hub.

Legal basis for processing personal information

We use a number of different legal bases for processing personal information and further information on this is provided in our *privacy notice* available on The Hub.

Where no other legal basis exists for processing an individual's personal data we will seek their consent. Any request for consent must be presented in a way that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language

An individual has the right to withdraw his or her consent at any time, and it must be as easy to withdraw consent as to give it in the first place.

Some examples and guidance regarding consent are shown in appendix A below.

Children and data protection

Children must be afforded particular protection when their personal information is being processed as they may be less aware of the risks involved.

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.

Where we rely on consent to process a child's personal data we must ensure the child understands what they are consenting to. When seeking consent we must recognise that there may be a perceived imbalance of power between the person requesting the consent and the child and we must ensure any imbalance is not exploited, even if this is unintended.

To ensure students' rights are protected, ordinarily:

- In our Prep schools we will seek a parents' consent to process a student's personal data.
- In our Senior Schools we will seek both the student and parents' consent to process a student's personal data, and may not treat this as true consent unless both agree.
- In our Sixth Forms, we will seek our students' consent to process their personal data.

The ICO provides further information on protecting the rights of children which may be found via a link on The Hub. Further advice may also be sought from the legal department or Data Protection Officer at Trust Office.

Security of personal information

Our information security policy deals with the confidentiality, integrity and availability of personal information and this policy may be found on The Hub.

Safe storage and safe sharing of personal information

Further information on the GDST 'golden principles' for the safe storage and safe sharing of personal information can be found on The Hub.

Clear desks

All staff are required to ensure that all confidential or restricted information in hardcopy or electronic form is kept secure, in particular:

- Computer workstations must be 'locked' when a workspace is unsupervised.
- Any Confidential or Restricted information must be removed from desks and locked in a drawer or filing cabinet when the desk is unoccupied and at the end of the work day.
- Filing cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not supervised.

Contracts with data processors

Whenever an arrangement is entered into with a data processor who will have responsibility for holding and/or processing GDST data, including personal data, a formal contract containing appropriate safeguards must be drawn up with that data processor that meets the standards outlined in Article 28 of GDPR.

Retention of personal information by staff on GDST systems

All staff are provided with a GDST Google and Microsoft Office 365 account, together with a GDST email account for use with, and storage of, information relating to GDST business.

Staff should not transfer digital content containing the personal information of students or parents, or work-related content containing the personal information of staff out of the GDST network, GDST approved third party applications, Google or Office 365 environment.

A 'digital first' culture is promoted within the GDST, and staff should not print paper records unless this is necessary.

The GDST retains the intellectual property rights (IP) of all material produced by GDST employees' during the course of their employment, and this material may not be retained or used for other purposes by individuals beyond their period of employment without the written permission of a line manager.

Asset management and data sanitisation

Further information concerning the GDST Asset Management and Data Sanitisation Policy can be found on The Hub.

Passwords

Further information concerning the GDST password policy can be found on The Hub.

Special Categories of Personal Information

The following activities involve the processing of special categories of personal information and additional guidance is provided to support this.

Medical records

Further information about the recording and storage of medical information in schools can be found on The Hub.

Safeguarding and Pastoral

Further information about the processing of personal information to support safeguarding and the provision of pastoral care can be found on The Hub.

Special educational needs and disability (SEND)

Further information about using personal information to support students with special educational needs or disability can be found on The Hub.

School trips

Further information about processing personal information for school trips can be found on The Hub.

Appendix A

Common data protection queries

Photograph commissioning agreement

A photograph commissioning agreement for external photographers is available on the knowledge section of the GDST Hub. This ensures that the school obtains copyright in all photographs commissioned, preventing the photographer from using the images of pupils without the school's consent. This should provide additional comfort to parents.

Publication of exam results

Schools should make sure that people are aware as early as possible whether examination results will be made public, and how this will be done.

This information should be repeated at regular intervals, for example at the start of each school year; or each examination term. Schools do not need students' consent to publish examination results, however they should consider any objections and then only publish results where there is a good reason to reject this objection.

Exam results

The Information Commissioner has issued specific guidance on the publication of exam results. Students may request information about their exam performance, including:

- marks;
- comments written by the examiner; and
- Minutes of any examination appeals panels

Students do not have a right to copies of answers given to exam questions.

Examples of issues surrounding consent

- School Trips — Consent in relation to a school trip must be sought from parents for the student to undertake the activity, not process personal data.

Having given consent to undertake the trip the school has a legitimate interest in processing personal information in support of this activity. This includes collating parent contact details, and an up-to-date photograph of the child in case they become lost. Consent is not required for this.

The school has a legal basis for processing personal information concerning health (for example allergies or medical conditions) in order to provide appropriate health care. This includes sharing information with authorised third parties (such as the trip venue). Consent is not required for this.

- Information sharing – safeguarding / Pastoral

The *HM Government information sharing advice for practitioners providing safeguarding services to children, young people, parents and carers July 2018* is non-statutory guidance on sharing information.

The Education (Independent School Standards) Regulations 2014 places a statutory responsibility on schools to safeguard and promote the welfare of children which includes sharing information where this is in the best interests of a child.

For further guidance or advice on sharing information with other agencies please speak to a member of the legal team.

- Photographs and CCTV

1. Photographs used to identify children in school records – we have a legitimate interest in obtaining these and consent is not required.

2. CCTV – where we use CCTV to ensure our schools are safe we do not need to seek consent as we have a legitimate interest in doing this. The ICO provides guidance on the use of CCTV which may be found on The Hub.

3. Photographs used to record classroom activity / dance / drama / sports within the school curriculum – we have a legitimate interest in recording students' work and academic progress, and do not need consent for this.

4. Photographs with images of multiple students used in school newsletters or magazines – where students are not readily identifiable, the legitimate interest of the school can be relied on and individual consent is not needed. Where images readily identify individual children, consent should be sought.

5. Marketing material or prospectuses – consent is needed where we wish to use a student's image for marketing purposes. We should not rely on the 'general photographic consent' and should seek a specific consent in these circumstances. Marketing staff should however consider the effect of consent being withdrawn. Where there is a significant financial outlay consideration may be given to a contractual arrangement.

- Biometric systems

Where a biometric system such as cashless catering or door access is proposed explicit consent must be sought.

	Where a student, parent or member of staff does not wish to consent to this an alternative system should be provided that does not disadvantage them in any way.
• School clubs / third parties	Where after school clubs or activities fall outside the national curriculum, we cannot rely on 'legitimate interest' as a basis for processing personal information and consent should be sought.