Policy lead(s): AS/AL	Creation Date: November 2016	Revision Due: October 2025
October 2018	KLW	
October 2019	KLW	
October 2020	KLW	
December 2021	KLW	
November 2022	KLW	
December 2024	AL	

WORKSOP COLLEGE AND RANBY HOUSE

Data Protection Policy

School Tier: Whole School including Ranby House Prep.

POLICY AIMS:

The law (the Data Protection Act 1998) changed on 25 May 2018 with the implementation of the General Data Protection Regulation (GDPR). This is an EU Regulation that is directly effective in Europe and following Brexit there are now two versions of the original EU GDPR including a separate version applicable in the UK. A new Data Protection Act 2018 was passed to deal with certain issues left for national law which included specific provisions of relevance to independent schools.

While this new law set out useful legal grounds in this area, in most ways it strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools and colleges that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law and has powers to act for breaches of the law.

This policy is intended to ensure that personal information is dealt with correctly and securely, and in accordance with UK GDPR 2021 and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

Introduction

At Worksop College and Ranby House we acknowledge the importance of data protection and recognise that individuals have rights in respect of the personal data we handle.

During the course of our business activities, we will collect, store, and process personal data. We will endeavour to treat this data in accordance with legal safeguards and in a manner consistent with the high standards individuals have come to expect from our organisation.

All our staff members are required to comply with this Data Protection Policy when processing personal data as part of their role. Failure to comply with this policy may lead to disciplinary action.

Policy lead(s): AS/AL	Creation Date: November 2016	Revision Due: October 2025
October 2018	KLW	
October 2019	KLW	
October 2020	KLW	
December 2021	KLW	
November 2022	KLW	
December 2024	AL	

The Senior Leadership Team is responsible for ensuring compliance with this policy in their respective areas of responsibility.

This policy is overseen by the GDPR and Compliance Manager.

Scope
This Data Protection Policy applies in respect of all the personal data we process about our current, past, and prospective students (and their parents/carers), our current and past staff members, our suppliers, and any third parties we communicate with.

This policy sets out how we will process personal data. The following policies are also relevant for this purpose:

- Privacy Notice
- Records Management and Retention Policy
- CCTV Policy
- Artificial Intelligence (AI) Policy

Data Protection Terms
For the purposes of this policy, the following terms apply:

Data Controller means the organisation that determines the purposes for processing personal data and the manner in which that processing will be carried out. Worksop College will be the data controller of the personal data it collects (for itself and Ranby House) and uses as part of its business activities.

Data processor means the organisation or person that processes personal data on our behalf and in accordance with our instructions, such as suppliers and contractors. Our staff members are not data processors.

Data subjects are all individuals about whom we hold personal data.

Personal data means any information relating to an individual who can be identified from that information or from any other information we may hold. Personal data can include names, identification numbers, addresses (including IP addresses), dates of birth, financial or salary details, educational background, job titles, and images. It can also include an opinion about an individual, their actions, or their behaviour. Personal data may be held on paper, on a computer, or in any other media, whether it is owned by the organisation or a personal device.

Processing means any activity that is performed on personal data or special category data. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, restriction, erasure, or destruction of data.

Special Categories of Personal Data are more sensitive and include information revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union

membership. It will also include data concerning health (physical and/or mental health), data concerning a person's sexual orientation, and genetic and biometric information where that data is used to uniquely identify a person. We will also treat data relating to criminal convictions or related proceedings in the same way as special categories of data.

Data Protection Principles
Worksop College and Ranby House are responsible for and must be able to demonstrate that personal data is being processed in accordance with the principles of the UK GDPR Data Protection Law. This is known as the duty of accountability (see below).

The principles of UK GDPR Data Protection Law are:

Principle One: Lawfulness, Fairness & Transparency
Personal data must be processed lawfully, fairly, and in a transparent manner.

In order to comply with this principle, we will ensure that we only process personal data where we are lawfully permitted to do so. We will be open and honest with individuals about the data we collect, why we use it, and which lawful basis justifies that use (see below). We will do this via privacy notices and policies, whether or not we collect information directly from the individuals concerned.

In addition, for each processing activity that we undertake, we will consider how that processing affects the individuals concerned.

In order to process data lawfully, we will ensure that at least one of the following lawful bases applies:

- The data has provided **consent**. This consent will be a freely given, specific, informed, and clear indication of the individual's wishes.
- The processing is necessary for the performance of a **contract** with the data subjects, such as the provision of education for a student under the parental contract.
- The processing is necessary for us to comply with a **legal obligation** (not a contractual obligation).
- Processing the data is necessary to protect an individual's **vital interests** (life or death), such as the management of a medical emergency.
- Processing is necessary to carry out a task in the **public interest** or where there is a clear basis in law.
- The processing is necessary for our **legitimate interests**, or those of a third party, so long as those interests are not overridden by the interests, rights, or freedoms of the data subject.

Principle Two: Purpose Limitation
Personal data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

In order to comply with this principle, we will only process personal data for the specific lawful purposes set out in our Record of Processing Activity and Privacy Notices, unless we are specifically permitted to process the data by law.

Policy lead(s): AS/AL	Creation Date: November 2016	Revision Due: October 2025
October 2018	KLW	
October 2019	KLW	
October 2020	KLW	
December 2021	KLW	
November 2022	KLW	
December 2024	AL	

Principle Three: Data minimisation
Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

In order to comply with this principle, the data we collect will be sufficient to fulfil the purpose of collection (adequate), there will be a rational link between that data and the purpose (relevant), and we will only collect the personal data we need to fulfil the specific purpose we have collected the data for (limited to what is necessary).

Principle Four: Accuracy
Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.

In order to comply with this principle, we will ensure that all personal data is kept up-to-date and is accurate. We have appropriate processes in place to check the accuracy of the data we collect, and the sources of data are always recorded. We will also comply with an individual's right to rectification (see below), and we will carefully consider any challenges to the accuracy of the personal data.

Principle Five: Storage Limitations
Personal Data shall be kept in a form which permits identification of Data Subjects for a period no longer than is necessary for the purposes for which the Personal Data is processed.

In order to comply with this principle, we will only keep personal data for as long as we need it, and we will take all reasonable steps to destroy or erase all data that is no longer required. Personal data will be kept in accordance with our Records Management and Retention policy to ensure that data is not kept any longer than necessary and we will ensure that individuals understand the duration for which their personal data will be held.

Principle Six: Integrity and confidentiality/security
Personal Data shall be 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.

In order to comply with this principle, we will ensure that we have appropriate organisational and technical measures in place to safeguard the security of the personal data we process. This includes ensuring the confidentiality, integrity, and availability of the systems and services used to process the personal data.

<u>Data Security</u>
We will ensure that we have appropriate security measures in place to protect personal data against unlawful or unauthorised processing and accidental loss or destruction.

In accordance with Principle Six (Integrity and confidentiality/security, above):

Policy lead(s): AS/AL	Creation Date: November 2016	Revision Due: October 2025
October 2018	KLW	
October 2019	KLW	
October 2020	KLW	
December 2021	KLW	
November 2022	KLW	
December 2024	AL	

- We will ensure the confidentiality of personal data by protecting it against unintentional, unlawful, or unauthorised access, disclosure, or theft.
- We will ensure the integrity of personal data by maintaining its accuracy and protecting it against accidental or unlawful alteration.
- We will ensure the availability of personal data by regularly testing, assessing, and evaluating the effectiveness of our technical and organisational measures to ensure our systems and services can be restored and accessed in a timely manner in the event of a physical or technical incident.

Our security measures include:

- Keeping personal data in paper records or on removable devices in lockable rooms, desks, or cupboards and disposing of these records securely when required.
- Keeping digital data in line with our agreed policies.
- Ensuring staff members only share personal data they use in the course of their work with authorised personnel.
- Maintaining up-to-date firewalls and other IT security measures, with regular audits of our IT systems.
- Training staff on the importance of data protection and safe handling of personal data.
- Regularly auditing our governance and information management processes.

Principle Seven: Accountability
The accountability principle requires that a Controller takes responsibility for what happens to personal data. Records and measures must be in place to demonstrate compliance.

In order to comply with this principle, we will take full responsibility for the personal data which we collect, use, store and destroy and adhere strictly to the other principles. We will maintain full and accurate records to demonstrate our use of the data.

Notifying Data Subjects
Where we collect personal data directly from individuals or via a third-party source, we will inform those individuals about the use of their data through our privacy notices, which will include the following details:

- The name and address of Worksop College as the data controller.
- The name and contact details of our GDPR and Compliance Manager.
- The categories of personal data we are processing.
- The purpose or purposes we intend to use the personal for.
- The legal basis for processing that personal data (and, where special categories of personal data are being processed, the additional processing condition allowing this).
- The recipients of any personal data we share or disclose.
- Details of any transfers to other countries and what safeguards are in place.
- The length of time we will retain the personal data.
- The rights data subjects have to access their data or limit its use or disclosure.

Policy lead(s): AS/AL	Creation Date: November 2016	Revision Due: October 2025
October 2018	KLW	
October 2019	KLW	
October 2020	KLW	
December 2021	KLW	
November 2022	KLW	
December 2024	AL	

- The right of data subjects to complain to the Regulatory Authority about our use of their personal data.
- The source of the personal data (where we receive it from a third party).
- The existence of any automated decision-making (including profiling).

Data Subject Rights
We recognise that data subjects have a number of rights regarding our use of their personal data, some of which are subject to conditions. All requests will be dealt with by our GDPR and Compliance Manager.

Right of access (commonly referred to as a subject access request - SAR)
This gives individuals the right to ask us about the personal data we use about them. This can include what we use it for, who we share it with, how long we store it and where we have obtained it from. Individuals can also ask for a copy of their personal data.

Right to rectification
This gives individuals the right to ask for inaccurate personal data to be corrected or for incomplete personal data to be completed.

Right to erasure ('right to be forgotten')
This gives individuals *the right* to ask for their personal data to be erased, but *the obligation* for us to erase personal data only applies in certain circumstances.

Right to object
This gives individuals the right to ask us not to use their data. This will include the use of their data for direct marketing or where automated decisions have been made about them.

Rights in relation to automated individual decision-making, including profiling
This gives individuals the right to object to decisions being made about them solely by automated means (without any human involvement) and to profiling (where automated processing is used to evaluate certain things about the individual).

If we are unable to comply with a request, then we will clearly inform data subjects about the reasons why.

Sharing and Transferring Personal Data
We will only transfer personal data to a data processor where they have provided us with sufficient guarantees that they will protect the data in compliance with data protection legislation and in line with our expectations. Where AI tools are used, and as required, we will obtain all relevant technical and functional documentation from the AI provider for our review before the tool is implemented. We will also ensure that these requirements are governed by a contract or other legally binding agreement.

The school will provide information to each pupil/parent (which can include relevant personal data of the respective parent and/or child) as necessary to facilitate school operations.

We will also enter into data sharing agreements with other data controllers, where this is considered appropriate.

Policy lead(s): AS/AL	Creation Date: November 2016	Revision Due: October 2025
October 2018	KLW	
October 2019	KLW	
October 2020	KLW	
December 2021	KLW	
November 2022	KLW	
December 2024	AL	

Data Retention and Disposal
We do not encourage the retention of any personal data for any longer than necessary, in accordance with Principle Five (Storage Limitation, above). We will ensure that all personal and special category data is disposed of in a way that protects the privacy of data subjects.

We will retain a Records Management and Retention policy that details the specific types of information we handle and the appropriate periods for retention.

Dealing with Data Protection Incidents
We will manage data protection incidents in accordance with the process set out by the ICO. As part of this process, we require all our staff members to follow a process of reporting any data incidents to the GDPR and Compliance Manager, and completing a data incident form, which we will investigate and log.

Data Protection Impact Assessments
We will carry out a Data Protection Impact Assessment when the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. This process is designed to identify the nature of the risks so that mitigating actions can be taken to reduce or eliminate these risks.

We have a process in place for our staff members to follow, which includes guidance about when a Data Protection Impact Assessment is required.

Use of CCTV
We use CCTV in accordance with our CCTV policy to ensure any images we collect and use are handled appropriately.

Use of Artificial Intelligence (AI)

We use educational and administrative AI tools, which we believe will enhance our students' experience at our schools. AI tools are used in accordance with our AI Policy.

Policy lead(s): AS/AL	Creation Date: November 2016	Revision Due: October 2025
October 2018	KLW	
October 2019	KLW	
October 2020	KLW	
December 2021	KLW	
November 2022	KLW	
December 2024	AL	