DJM/2018

DATA PROTECTION POLICY

Statement of intent

Redborne Upper School is required to keep and process certain information about its pupils, staff members and other contacts in accordance with its legal obligations under the General Data Protection Regulation (GDPR). The school may, from time to time, be required to share personal information about its pupils, staff members and other contacts with other organisations, mainly the LA, other schools and educational bodies, and potentially social services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR. Organisational methods for keeping data secure are imperative, and Redborne Upper School believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018.

Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

Guidelines

1 Registers and Records

The school has registered with the Data Protection Registrar under the Data Protection Act 1998.

2 The Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial 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; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- 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, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- 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.
- The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

3 Personal Data

Definitions of personal data are complex, and it is difficult to define categorically. However, broadly speaking and in day to day use, "personal data" is information which relates to a living, identifiable individual.

In the context of this document and the school's requirement to process "personal data" as part of its duty of care and to educate its students, "personal data" may include:

- School admission and attendance registers
- Student's curricular records
- Reports to parents or carers on the achievements of their children
- Records in connection with students entered for prescribed public examinations
- Staff records, including payroll records
- Student disciplinary records
- Personal information for teaching purposes
- Records of contractors and suppliers
- Photographic and video documentation

Furthermore, "personal data" extends to online identifiers, such as IP addresses and usernames. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudo-anonymised data, e.g. key-coded.

4 Processing Personal Data

If it is necessary for the school to process certain personal data to fulfil its obligations to students and their parents or carers then consent is not required. However, any information which falls under the definition of personal data, and is not otherwise exempt will remain confidential. Data will only be disclosed to third parties with the consent of the appropriate individual or under the terms of this Policy.

5 Sensitive Personal Data

Sensitive personal data is referred to in the GDPR as 'special categories of personal data', these may include:

- Ethnic or racial origin
- Political opinions
- Religious beliefs
- Other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health condition
- Sexual life
- Offence or alleged offence
- Proceedings or court sentence
- Genetic data
- Biometric data
- Data concerning health matters.

Sensitive personal data shall only be processed subject to the conditions set out in Article 9(2) of the GDPR.

6 Accountability

Redborne Upper School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

The school will provide comprehensive, clear and transparent privacy policies for key stakeholders; these are included at the end of this document as:

- Appendix A - Student Privacy Notice
- Appendix B – Staff Privacy Notice
- Appendix C – Contact Privacy Notice

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation
- Pseudo-anonymisation
- Transparency
- Allowing individuals to monitor processing
- Continuously creating and improving security features

7 Data protection officer (DPO)

A DPO will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members
- The role of DPO will be met in-house provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests
- The DPO will report to the highest level of management at the school, which is the Headteacher
- The DPO will operate independently and will not be penalised for performing their task
- Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

8 Rights of Access

Individuals have a right of access to information held by the school. Any individual wishing to access their personal data should submit a Subject Access Request (SAR) in writing addressed to the Headteacher.

- The school will verify the identity of the person making the request before any information is supplied.
- A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.
- Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
- Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
- All fees will be based on the administrative cost of providing the information.
- All requests will be responded to without delay and at the latest, within one month of receipt.
- In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
- Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.
- In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

It is important to note that certain data is exempt from the right of access under the Data Protection Act. This can include:

- Information which identifies other individuals
- Information which the school reasonably believes is likely to cause damage or distress
- Information which is subject to legal professional privilege

The school will also treat as confidential any reference given by the school for the purpose of the education, training or employment, or prospective education, training or employment of any student. The school acknowledges that an individual may have the right to access a reference relating to them received by the

school. However, such a reference will only be disclosed if doing so does not identify the referee or where the referee has given their consent or if disclosure is considered reasonable.

9 Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained – please refer to section 9.

Furthermore, processing must be necessary for:

- Compliance with a legal obligation
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- For the performance of a contract with the data subject or to take steps to enter into a contract
- Protecting the vital interests of a data subject or another person
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.
- Carrying out obligations under employment, social security or social protection law, or a collective agreement
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Reasons of substantial public interest which is proportionate to the aim pursued and which contains appropriate safeguards
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject.

10 Consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of

the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given, this record may be electronic or paper based.

The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent can be withdrawn by the individual at any time.

11 The right to be informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge

If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and where applicable, the controller's representative and the contact details of the DPO.
- The purpose of, and the legal basis for, processing the data
- The legitimate interests of the controller or third party (if applicable)
- Any recipient or categories of recipients of the personal data
- Details of transfers to third countries and the safeguards in place
- The retention period of criteria used to determine the retention period.
- The existence and location of this policy and so the other rights of the individual outlined herein

12 The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the school will inform the third party of the rectification where possible. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

13 The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child.

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

14 The right to restrict processing

Individuals have the right to block or suppress the school's processing of personal data. In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The school will inform individuals when a restriction on processing has been lifted.

15 The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Please note that personal data will be provided in a structured, commonly used and machine-readable form and will be provided free of charge. Where feasible, data will be transmitted directly to another organisation at the request of the individual however Redborne Upper School is not required to adopt or maintain processing systems which are technically compatible with other organisations (GDPR Recital 68).

In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

The school will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

16 The right to object

The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information. Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.
- Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

17 Disclosure of Information

The school confirms that it will not generally disclose information about individuals, unless the individual has given their consent or one of the specific exemptions applied under the legislation set out in the "Legal Framework" section of this policy. However, for the following purposes, the school does intend to disclose data as is necessary to third parties:

- To give confidential references for any educational institution which the student may wish to attend
- To publish the results of public examinations or other achievements of students of the school
- To disclose medical details of a student's medical condition whether it is in the student's interests to do so (eg to organisers of a school trip)

When the school receives a disclosure request from a third party it will always take action to establish the identity of that third party before making any disclosure.

18 Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Headteacher will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

19 Security

Where it is reasonably practicable, the school will take steps to ensure that members of staff will only have access to personal data relating to students, their parents or carers when it is necessary for them to do so. All staff will be made aware of this policy and their duties. The school will ensure that all personal information is held in a secure central location and is not accessible to unauthorised persons.

In addition to this:

- Confidential paper records will be kept in a secure and locked location.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Access to digital data limited; staff computers use full disk encryption and restricted permissions are in place on servers to prevent access except where necessary based on the principle of least privilege.
- Where data is saved on removable storage or a portable device, the device will be kept in a secure and locked location when not in use.
- Memory sticks will not be used to hold personal information unless such information is encrypted.
- All electronic devices are password-protected to protect the information on the device and the wider network in case of theft.
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- All necessary members of staff are provided with their own secure login and password. Staff passwords must adhere to complexity requirements, with a maximum age for passwords also enforced.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Staff will be required to take part in training to ensure they are aware of their obligations with regards to this policy, in particular:

- Their duty to protect personal data, including but not limited to ensuring unattended paper records are secured, other users are not given access to electronic devices using staff access rights and unattended electronic devices are locked
- The additional risks and how to mitigate them when accessing school material on personal devices including the how to encrypt devices, ensuring that only they have access to these accounts and that data is not stored on these devices.

Staff will be asked to read key policy and training documents, including updates, and will be required to indicate by signing an IT agreement that they both understand and are complaint with these requirements.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

20 Data Retention

Data will not be kept for longer than is necessary and it is the intention of the school to implement the guidance outlined by the Department for Education, summarised in Appendix D.

The school has historically retained data for 25 years; restrictions in the current capability of the MIS used by the school prevent practical deletion of this historic data. The school will continue to work with its supplier to enact this guidance as soon as possible and it is anticipated that this should be complete by January 2019 when this policy will be reviewed. In the interim, data which cannot practically be erased in bulk will be subject to deletion requests on request.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

21 Enforcement

If an individual believes that the school has not complied with this Policy or acted otherwise than in accordance with the legislation set out in the "Legal Framework" section, they should make a complaint to the school and notify the Data Protection Officer.

22 Key Staff

There are a number of individuals with key responsibilities in relation to data protection, these are:

Role	**Name(s)**
Head of centre	Steve Gray
Data Protection Officer	Andrew French
IT Network Manager	Jamie Thompson
Data Manager	Ian Belcher
Exams Officer	Donna Nunn
Exams Officer Line Manager (Senior Leader)	Andrew French

Should you wish to contact any of these staff, please use the main school contact details and your queries will be redirected as appropriate. Details are available on the school website.

23 Examinations

As a school one of the key areas of information exchange is in connection to examinations; this section outlines specific requirements in relation to this role.

There is a requirement for the exams office(r) to hold exams-related information on candidates taking external examinations. If you wish to determine the information held you are entitled to make a Subject Access Request (SAR) as outlined in section 8 above.

Candidates' exams-related data may be shared with the following organisations:

- Awarding bodies
- Joint Council for Qualifications
- Department for Education
- Local Authority

This data may be shared via one or more of the following methods:

- hard copy
- email
- secure extranet site(s)
- encrypted electronic storage devices

This data may relate to exam entries, access arrangements, the conduct of exams and non-examination assessments, special consideration requests and exam results/post-results/certificate information.

Monitoring, Evaluation and Review

This policy will be monitored, evaluated and reviewed every three years by the senior leadership team.

Dissemination of the Policy

This policy is available on the school website, on request to parents and carers, the LA and Ofsted through the Headteacher.

Date approved by governors	
Date for review	January 2019

APPENDIX A: Student Privacy Notice - How we use pupil information
May 2018

The school is the Data Controller for the purposes of the General Data Protection Regulation. This means we collect information from you, and receive information about your son or daughter from their previous school. We hold this data and use it to support your son or daughter's learning; monitor and report on their progress and provide appropriate pastoral care.

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as predicted grades, exam results)
- Relevant medical information (such as medical conditions)
- Special educational needs information (such as an Education, Health and Care Plan)
- Exclusions / behavioural information (such as detentions, achievement points)
- Course and timetable information (such as which options are taken)

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

The lawful basis on which we use this information

We collect and use pupil information under section 537A of the Education Act 1996, and section 83 of the Children Act 1989. We also comply with Article 6(1)(c) and Article 9(2)(b) of the General Data Protection Regulation (GDPR).

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

APPENDIX A: Student Privacy Notice - How we use pupil information
May 2018

Storing pupil data

Data will not be kept for longer than is necessary and it is the intention of the school to implement the guidance outlined by the Department for Education, summarised in the schools data protection policy.

The school has historically retained data for 25 years; restrictions in the current capability of the MIS used by the school prevent practical deletion of this historic data. The school will continue to work with its supplier to enact this guidance as soon as possible and it is anticipated that this should be complete by January 2019 when this policy will be reviewed. In the interim, data which cannot practically be erased in bulk will be subject to deletion requests on request.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- NHS
- contracted organisations

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services

Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

APPENDIX A: Student Privacy Notice - How we use pupil information
May 2018

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

APPENDIX A: Student Privacy Notice - How we use pupil information
May 2018

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact:

Andrew French, Data Protection Officer, dataprotection@redborne.com.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact:

Andrew French, Data Protection Officer, dataprotection@redborne.com.

APPENDIX B: Staff Privacy Notice - How we use workforce information
May 2018

The school is the Data Controller for the purposes of the General Data Protection Regulation. This means we collect information from you.

The categories of school information that we process include:

- personal information (such as name, employee or teacher number, national insurance number)
- characteristics information (such as gender, age, ethnic group)
- contract information (such as start date, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- performance management (such as annual reviews, targets)
- pension information (such as contributions, length of employment)

Why we collect and use workforce information

We use workforce data to:

a) enable the development of a comprehensive picture of the workforce and how it is deployed
b) inform the development of recruitment and retention policies
c) enable individuals to be paid
d) enable effective performance management
e) enable continued professional development
f) ensure individuals receive an appropriate pension

Under the General Data Protection Regulation (GDPR), the legal basis / bases we rely on for processing personal information for general purposes are:

Section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments, article 6(1)(c) and Article 9(2)(b) of the General Data Protection Regulation (GDPR).

Collecting workforce information

We collect personal information via new employment forms as well as any updates therein.

Workforce data is essential for the school's / local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information

Data will not be kept for longer than is necessary and it is the intention of the school to implement the guidance outlined by the Department for Education, summarised in the schools data protection policy.
The school has historically retained data for 25 years; restrictions in the current capability of the MIS used by the school prevent practical deletion of this historic data. The school will continue to work with its supplier to enact this guidance as soon as possible and it is anticipated that this should be complete by January 2019 when this policy will be reviewed. In the interim, data which cannot practically be erased in bulk will be subject to deletion requests on request.

APPENDIX B: Staff Privacy Notice - How we use workforce information
May 2018

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

Who we share workforce information with

We routinely share this information with:

- our local authority (where applicable)
- the Department for Education (DfE)
- pension providers

Why we share school workforce information

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections.

We are required to share information about our school employees with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Andrew French, Data Protection Officer, dataprotection@redborne.com

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

APPENDIX B: Staff Privacy Notice - How we use workforce information
May 2018

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact: Andrew French, Data Protection Officer, dataprotection@redborne.com.

How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Sharing by the Department

The Department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

To contact the department: https://www.gov.uk/contact-dfe

APPENDIX C: Contact Privacy Notice - How we use parental/guardian/contact information May 2018

The school is the Data Controller for the purposes of the General Data Protection Regulation. This means we collect information from you.

The categories of information that we collect, hold and share include:

- Personal information (such as name and address)

Why we collect and use this information

We use the data:

- to contact parent/guardian/named contact in the case of an emergency
- provide feedback of their child's progress in school
- to enable parents to interact electronically with the school (such as through apps and websites)

The lawful basis on which we use this information

We comply with Article 6(1)(c) and Article 9(2)(b) of the General Data Protection Regulation (GDPR).

Collecting parent/guardian/contact information

In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain information to us or if you have a choice in this.

Storing parent/guardian/contact data

Data will not be kept for longer than is necessary and it is the intention of the school to implement the guidance outlined by the Department for Education, summarised in the schools data protection policy.

The school has historically retained data for 25 years; restrictions in the current capability of the MIS used by the school prevent practical deletion of this historic data. The school will continue to work with its supplier to enact this guidance as soon as possible and it is anticipated that this should be complete by January 2019 when this policy will be reviewed. In the interim, data which cannot practically be erased in bulk will be subject to deletion requests on request.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

Who we share parent/guardian/contact information with

We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- contracted organisations

Why we share parent/guardian/contact information

We do not share information about parents/guardians/contacts with anyone without consent unless the law and our policies allow us to do so.

APPENDIX C: Contact Privacy Notice - How we use parental/guardian/contact information May 2018

Requesting access to your personal data

Under data protection legislation, parents/guardians/contacts have the right to request access to information about them that we hold. To make a request for your personal information, contact:

Andrew French, Data Protection Officer, dataprotection@redborne.com.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact:

Andrew French, Data Protection Officer, dataprotection@redborne.com.

APPENDIX D: Department for Education Guidance on Data Retention

The following table outlining data retention recommendations was obtained from the Department for Education on 10/05/2018:

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
Admissions		Admissions files	Admissions appeals		**Admissions files** Admissions data is used extensively from the period of the school receiving it up until the point where children enrol. It is then used for some validation and cross checking of enrolment details. Once enrolled, the child's records in the MIS become the core record. Data about children who enrolled but didn't get in is useful, but any intelligence gathered from it (for example, where in the city children are interested in our school, or the SEN make up) is aggregated within the first year to a level being non-personal, after that, the detailed data within the admission file could be deleted. It is important to retain detailed data for a year, any appeals for which richer data about other successful/unsuccessful appeals may be relevant typically happen in the first year. **Information about admissions appeals** When dealing with appeals, having a reasonable history of any other appeals in some detail can be needed to deal with the particular appeal. The information is needed alongside the admissions policies of the time.

APPENDIX D: Department for Education Guidance on Data Retention

Attainment			X		Formative assessment data is useful as a child is building towards a particular more formal assessment. Once the child leaves the school, it has little value in terms of retention. Summative attainment is the main outcome of what children 'attain' in school. It is important that future schools where pupils go on to learn can understand previous attainment. Whilst often that information is 'passed on' smoothly as children move phase, it is not always the case, and thus retaining the names alongside the main attainment data for 1 year after the pupil has left the school feels proportionate. Trend analysis is important, 3 to 5 years is often the 'trend' people look at, but longer may be relevant. Whilst this must be fully flexible in reporting small sub groups, and the data would wish to be retained at individual level, some personal data (for example, name) could be removed from the data to reduce sensitivity. After 3 to 5 years, then aggregated summaries that have no risk of identifying individuals are all that are typically needed to be retained.
Attendance		X			Attendance data probably resides in some 'operational' systems in schools, such as cashless catering. In these systems, the data should only be retained until the associated business processes have concluded (for example, payment of meals). The start of the next academic year once all bills are settled feels proportionate. Attendance is related to individual attainment

APPENDIX D: Department for Education Guidance on Data Retention

					and so being able to relate attendance to attainment whilst in our care is important. Keeping it in detailed, individual form for one year after the pupil leaves school support conversations about detailed attendance that may be needed to best support that child. After that period, non-identifiable summary statistics are all that is required to support longer-term trend analysis of attendance patterns. We noted another GDPR principle here that may apply to attendance. Under data minimisation, where 'paper records' capture attendance, this paper record duplicates the electronic version and is probably required once the paper has been transferred to a stable electronic format.
Behaviour		X			This is all relevant for managing children when with at your school. 1 year allows a period of 'handover' to next institution with conversations supported by rich data if relevant.
Exclusions		X			Exclusion data should be 'passed on' to subsequent settings. That school then has responsibility for retaining the full history of the child. If a private setting or the school is unsure on where the child has gone, then the school should ensure the LA already has the exclusion data.
Identity management and authentication	X (images used for identity management)				

APPENDIX D: Department for Education Guidance on Data Retention

Catering and free school meal management	X (meal administration)	X (free school meal eligibility information)	Catering and free school meal management		A short historic record of what a child has had may be useful in case of any food-related incidents at school, or parental queries about the types of meals their children are choosing. Keeping for up to one year also allows time to do accounting work associated with catering. Typically 'one month' may not be enough, but 'one year' feels enough. Due to the way school funding works, free school meal eligibility is a financial matter, and thus keeping this data for 6+1 feels appropriate. This 7-year record also needs to be portable with the pupil, as historic dates can be used for funding.
Trips and activities	X (field file) X (educational visitors into school)		X (financial information related to trips)	X (major medical events)	Financial information related to trips should be retained for 6 years + 1 for audit purposes. This would include enough child identifiers to be able to confirm contributions. A 'field file' is the information that is taken on a trip by a school. This can be destroyed following the trip, once any medicines administers on the trip have been entered onto the core system. If there is a minor medical incident (for example, a medical incident dealt with by staff in the way it would be dealt with 'within school') on the trip, then adding it into the core system would be done. If there is a major incident (for example, a medical incident that needed outside agency) then retaining the entire file until time that the youngest child becomes 25 would be appropriate.

APPENDIX D: Department for Education Guidance on Data Retention

					Permission to go on the trip slips will contain personal data, and destroying them after the trip unless any significant incident arises is appropriate, otherwise refer to the policies above. Schools sometimes share personal data with people providing 'educational visits' into school. There should be good policies in place to ensure that the sharing is proportionate and appropriately deleted afterwards.
Medical information and administration	X (permission slips)	X (medical conditions and ongoing management)		X medical incidents (potentially)	To support any handover work about effective management of medical conditions to a subsequent institution. Permission forms that parents sign should to be retained for the period that medication is given, and for 1 month afterwards if no issue is raised by child/parent. If no issue is raised in that time, that feels a reasonable window to assume all was administered satisfactorily. Adding this policy to the permission slip would seem prudent. Medical 'incidents' that have a behavioural or safeguarding angle (including the school's duty of care) should refer to the retention periods associated with those policies.
Safeguarding				X	All data on the safeguarding file potentially forms part of an important story that may be needed retrospectively for many years. The elements of a pupil file (name, address) that are needed to identify children with certainty are needed to be retained along with those records.

APPENDIX D: Department for Education Guidance on Data Retention

Personal identifiers, contacts and personal characteristics	X (images used in identity systems) X (biometrics) X (house number and road)	X (images used in displays in school)	X (postcodes) X (names) X (characteristics)		Images are used for different reasons, and the reason should dictate the retention period. Images used purely for identification can be deleted when the child leaves the setting. Images used in displays etc. can be retained for educational purposes whilst the child is at the school. Other usages of images (for example, marketing) should be retained for and used in line with the active informed consent captured at the outset of using the photograph. Biometric data (typically fingerprints used in things like catering) should be used and retained as set out in the active informed consent gained at the outset, but typically this should not be retained long after the activity that requested its use has finished (for example, the child no longer attends the school to have a meal). As set out in other sections, names are needed for smooth handover to subsequent schools for up to one year. Postcode data is useful in analysing longer-term performance trends or how catchment/pupil populations are shifting over time, but full address data (house number and road) is not required for that activity. Schools may well provide references for pupils for up to 3 years after they leave, and so retaining the name in the core pupil record is important (this doesn't mean it needs to be retained in all systems). Keeping names attached to safeguarding files for longer than this may be entirely appropriate – see safeguarding section.

APPENDIX D: Department for Education Guidance on Data Retention

					Characteristics form an essential part of trend analysis, and so retention is in line with those needs.