Royds

Data Protection Policy

Aspiration: Dream Big
If your dreams don't scare you, they aren't big enough!

Resilience: Be Determined
Resilience is a skill, not an ability. It can be learnt.

Respect: Communicate with Kindness
Manners cost nothing but mean everything.

Initiative: Solve Problems
Every problem is a gift – without problems we would not grow.

Reflective: Never Stop Learning
Never stop learning because life never stops teaching.

Approved on 16th April 2018

1. Introduction

Royds School will comply with the requirements of the General Data Protection Regulations 2018 (GDPR). Staff who are involved with the collection, processing and disclosure of personal information have been made aware of their duties and responsibilities within this policy.

The school takes its obligations as a Data Controller very seriously and ensures that it treats personal information lawfully and correctly.

2. Personal Data

Personal data is defined within the GDPR as:

> *"Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier."*

This means that personal data includes any reference to a person by:

- Name
- Initials
- An ID number like a UPN or candidate number
- Location both physical or electronic like an IP address
- Image
- Biometric or genetic identifiers
- Any other pseudonym

Article 5 of the GDPR outlines requirements the school adheres to when processing personal data. Data is:

a. processed lawfully, fairly and in a transparent manner in relation to individuals
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d. accurate and, where necessary, kept up to date. See Appendix A.
e. 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.
f. 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.

2.1 Special Category Personal Data

Article 9 of the GDPR defines "special categories of personal data". This specifically includes:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)

- health
- sex life
- sexual orientation.

Where special category data is processed, an additional condition of processing must be met as these types of personal data pose a more significant risk to a person's rights and freedoms. The additional criteria are:

a. explicit consent. The school will always seek such consent in writing e.g. for permission to store biometric information for cashless catering.
b. carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law.
c. to protect the vital interests of the data subject.
d. processing is carried out in the course of its legitimate activities.
e. processing relates to personal data which are manifestly made public by the data subject.
f. processing is necessary for the establishment, exercise or defence of legal claims.
g. processing is necessary for reasons of substantial public interest.
h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional.
i. reasons of public interest in the area of public health.
j. archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

2.2 Criminal Offence Data

The GDPR rules for special category data do not apply to information about criminal allegations, proceedings or convictions. There are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, set out in Article 10. This specifies that the school can only keep a comprehensive register of criminal convictions if doing so under the control of official authority.

The school's safeguarding obligations arise from a legal duty to perform safer recruitment checks and to safeguard children once adults are working with them. Criminal offence data is only used in this area.

3. Lawful Processing Basis

The GDPR specifies that before any processing takes place, the lawful bases for processing the data has been identified. There are six bases are:

a. **consent**: the individual has given clear consent for the school to process their personal data for a specific purpose.
b. **contract**: the processing is necessary for a contract the school has with the individual, or because they have asked the school to take specific steps before entering into a contract.
c. **legal obligation**: the processing is necessary for the school to comply with the law.

d. **vital interests**: the processing is necessary to protect someone's life.
e. **public task**: the processing is necessary for the school to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.
f. legitimate interest: the processing is necessary for the school's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Where special category personal data is processed, a further condition for processing the data must also be met. Data will not be processed for a purpose other than that specified without informing individuals.

The school has a comprehensive Information Asset Register which documents the legal basis for identified processing activities. This is reflected in school privacy notices.

3.1 Consent

The school recognises that there is an in-balance of power between a large organisation and an individual and so consent is rarely used as a processing base. Where the school does process personal data based on consent, individuals have a genuine choice and the option to withdraw this at any time without being disadvantaged in any way. Consent can be withdrawn by submitting a Withdrawal of Consent form (Appendix C).

The majority of the school's processing activities fall under alternate lawful processing bases. Consent is generally relied on for discretionary processing activities such as marketing or PR.

Where express consent is relied on for a processing activity of special category data (e.g. biometric cashless catering permission), this will always be sought in writing.

3.2 Contract

The school will rely on a contract to process personal data usually for members of staff with employment contracts, organisations where a contract or service level agreement exists or for incidental activities where there is a reasonable expectation that a contract exists in contract law, such as purchasing goods. It should be noted that the school will not always require a written contract as a formal signed document.

3.3 Legal Obligation

A large number of the school's processing activities stem from a legal basis. The GDPR requires that the legal obligation must be laid down by UK or EU law although this does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it.

Although this list is not definitive, the majority of our legal obligations stem from:

- Health and Safety Act 1974
- Rehabilitation of Offenders Act 1974 (Exceptions) (Amendment) (England and Wales) Order 2012
- Limitation Act 1980
- Childrens Act 1989 and 2004
- Control of Asbestos at Work Regulations 1996 and 2012
- Education Act 1996, 2002 and 2011
- The Control of Substances Hazardous to Health Regulations 1997 and 2002
- School Standards and Framework Act 1998
- Terrorism Act 2000 and CTSA 2015

- Education (Health Standards) (England) Regulations 2003
- Education (Pupil Information) Regulations 2005
- Regulatory Reform (Fire Safety) Order 2005
- Education and Inspections Act 2006
- The Education (Pupil Registration) (England) Regulations 2006, 2010, 2011, 2013 and 2016
- Safeguarding Vulnerable Groups Act 2006
- Education and Skills Act 2008
- School Information (England) Regulations 2008
- Children and Young Persons Act 2008
- Designated Teacher (Looked After Pupils etc) Regulations 2009
- School Staffing (England) Regulations 2009
- Equality Act 2010
- Education (School Teachers' Appraisal) (England) Regulations 2012
- Teachers' Disciplinary (England) Regulations 2012
- Children and Families Act 2014
- Care Act 2014
- Special Educational Needs and Disability Regulations 2014
- School Governance (Constitution and Federations) (England) (Amendment) Regulations 2016

3.4 Vital Interests

Vital interests apply when the processing is necessary to protect a person's life and so is limited in scope. This is not a legal base that the schools will use other than in exceptional circumstances relating to emergency medical care.

3.5 Public Task

This is used where the processing is necessary for the school to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law. The GDPR states that public authorities do not need specific legal authority for the particular processing activity providing the overall purpose must be to perform a public interest task or exercise official authority, and that overall task or authority has a sufficiently clear basis in law.

3.6 Legitimate Interest

Legitimate interest processing is when personal data is

- processed in ways people would reasonably expect and which have a minimal privacy impact.
- where there is a compelling justification for the processing.
- where there can be broader benefit to society or a third party.

It is not usually appropriate for public authorities and so the school avoids processing on this basis. Where processing would take place on this basis, a Legitimate Interest Assessment (LIA) (Appendix D) will take place.

4. Individual Rights

The GDPR strengthens the rights that individuals have over their data. The school understands its obligations to individuals and has designed appropriate systems to support these rights. When requests are made verbally under these rights, school staff will complete the appropriate form on behalf of the applicant.

4.1 Right to be Informed

A key transparency requirement under the GDPR is that individuals have the right to be informed about the collection and use of their personal data. All school privacy notices are concise, transparent, intelligible, easily accessible and use clear and plain language. When collecting personal data from individuals, we will inform them of the purposes for which it is being processed and if it is being shared with any third parties.

4.2 Right of Access

Under GDPR, individuals have the right to know that their data is being processed, access to their data and to any additional supplementary information. This is to allow them to verify the lawfulness of the processing.

4.2.1 Subject Access Request Process

1. To make a request, individuals should use the Subject Access Request form (Appendix E) unless they have a disability which prevents them from doing so.
2. Reasonable steps will be undertaken to verify a person's identification and rights to the data.
3. The information requested will be provided in the format that it was requested e.g. if the request was made electronically then the information will be provided in a commonly used electronic format.

4.2.1 Subject Access Request Additional Information

Royds School will make no charge for providing the information to individuals unless. The only time an administrative fee will be charged will be when a request is manifestly unfounded or excessive, particularly if it is repetitive. A reasonable fee may also be charged to comply with requests for further copies of the same information.

Information will normally be provided without delay and at the latest within one month of receipt. The only exception will be where requests are complex or numerous and there will be an extension the period of compliance by a further two months. If this is the case, the school will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the school will:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where the school refuses to respond to a request, it will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

4.3 Right of Rectification

The school makes every effort to ensure that the data it holds is accurate and correct. Under GDPR, individuals have the right to have inaccurate data rectified. They are also entitled to have incomplete personal data completed. Where incorrect information has been passed to a third party, the school will make every effort to rectify this. Errors will be resolved within one month although usually it will be quicker than this.

Where errors are discovered in the data that the school holds, although verbal requests will be accepted, these should normally be notified using the Personal Data Rectification Form (Appendix A) and this will be considered.

The right to rectification applies primarily to factual personal data and subjective data (e.g. grades awarded) will not normally be considered under this right. Where there is a dispute over the accuracy of the school's data and the school has investigated the request and disagrees with the assertion that the data held is incorrect, the individual will be informed of this. The decision will be explained and the individual informed of their right to make a complaint to the ICO or another supervisory authority and their ability to seek to enforce their rights through a judicial remedy.

4.4 Right of Erasure

GDPR gives individuals have the right to have personal data erased in certain circumstances. This right applies when:

- the personal data is no longer necessary for the purpose which it was originally collected or processed.
- an organisation is relying on consent as the lawful basis for holding the data, and the individual withdraws their consent.
- an organisation is relying on legitimate interests as the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing.
- an organisation processed the personal data for direct marketing purposes and the individual objects to that processing.
- an organisation processed the personal data unlawfully.
- an organisation has to do it to comply with a legal obligation.
- an organisation processed the personal data to offer information society services to a child.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information.
- to comply with a legal obligation.
- for the performance of a task carried out in the public interest or in the exercise of official authority.
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing.
- for the establishment, exercise or defence of legal claims.

The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest
- if the processing is necessary for the purposes of preventative or occupational medicine e.g. where the processing is necessary for the working capacity of an employee

The majority of the school's processing activities fall within a legal obligation or a public duty so would not be subject to the right to erasure. Requests will be considered (Appendix F) however they will only be successful if they meet one of the above criteria.

When rejecting a request, an individual will be informed in a timely manner and within one month of receipt of the request. The following will be explained:

- the reasons for not complying with the request.
- their right to make a complaint to the ICO or another supervisory authority.
- their ability to seek to enforce this right through a judicial remedy.

When data is erased other organisations will be notified and erased from any public online environments.

4.5 Right of Restrict Processing

The GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that the school uses their data. This is an alternative to requesting the erasure of data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they dispute the content of the information held or how their data has been processed. In most cases, processing may be subject to a temporary restriction while these issues are resolved.

Individuals have the right to request processing is restricted in the following circumstances:

- the individual contests the accuracy of their personal data and you are verifying the accuracy of the data.
- the data has been unlawfully processed and the individual opposes erasure and requests restriction instead.
- The school no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim.
- the individual has objected to the school processing their data and the school is considering whether legitimate grounds exist to override those of the individual.

When an individual requests restriction of processing (Appendix G), the school will put measures in place to facilitate this. It may include:

- temporarily moving the data to another processing system.
- making the data unavailable to users.
- temporarily removing published data from a website.
- informing staff that they may not process any data relating to that individual.
- protecting archived data from disposal
- informing other organisations who the data has been shared with.

Restricted data will not be processed further in any way except to store it unless:

- the individual has given consent.
- it is for the establishment, exercise or defence of legal claims.
- it is for the protection of the rights of another person (natural or legal).
- it is for reasons of important public interest.

Once the school has made a decision to resolve the individual's issue with their data, the school may decide to lift the restriction. In this situation the individual will be informed prior to the restriction being removed.

4.6 Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. Schools already do this under the Common Transfer File system and there are legal obligations to share child protection information. This means the majority of data will automatically move when a student goes to another school.

If any further information is required to be transferred, a Data Portability Request form (Appendix H) should be completed.

4.7 Right to Object

GDPR gives individuals the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling).
- direct marketing (including profiling).
- processing for purposes of scientific/historical research and statistics.

Should an individual wish to object, they can do so on an Objection to Personal Data Processing Form (Appendix I).

4.8 Rights Related to Automated Decision Making Including Profiling

The GDPR gives individuals rights in relation to automated individual decision-making (making a decision solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain things about an individual).

Royds School does not use either profiling or automated decision making.

5. Governance Arrangements

Accountability and transparency are core principles of the GDPR and the school has designed data systems and security systems with these principles at their heart by implementing comprehensive but proportionate governance measures. These include:

- a culture of data security amongst staff
- data protection policies
- staff training
- internal audits of processing activities,
- reviews of internal HR policies;
- maintain relevant documentation on processing activities through the Information Asset Register (IAR)

- appointing a Data Protection Officer;
- implement measures that meet the principles of data protection by design and data protection by default.

5.1 Documentation

The GDPR places a requirement on organisations with over 250 employees to maintain certain types of documentation. Although this does not oblige the school to do so, documentation has been prepared as a matter of good governance due to the frequency and scale of processing activities.

The following information is available:

- The name and contact details of the school organisation and, where applicable, of other controllers, the school's Data Protection Officer is documented in all school privacy notices.
- The Information Asset Register (IAR) and, where applicable associated privacy notices, document:
    - the purpose of processing.
    - a description of the categories of individuals and categories of personal data.
    - The categories of recipients of personal data.
    - Details of any transfers to third countries including documenting the transfer mechanism safeguards in place.
- The IAR also includes records of consent, the existence of controller-processor contracts, the location of personal data, any Data Protection Impact Assessments and records of breaches.
- The Records Management Policy has a comprehensive retention scheme which is reflected in the Information Asset Register where appropriate.
- The Information Security Policy documents the schools organisational and technical security measures.

5.2 Contracts

The GDPR makes data controllers liable for the activities of their processors. As a data controller, the school will only use data processors who are able to provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected.

The school has a comprehensive Information Asset Register (IAR) which documents processing activities and the legal bases for processing. As part of this any third party sharing has been documented and contracts have been put in place with third parties (Appendix J). Where processors use a sub-processor, they have an obligation to inform the school and seek consent as well as putting a contract in place.

6. Data Protection by Design

The school is obliged under GDPR to design systems and processes with privacy by design at the heart of them. All new significant processes and technical systems from May 2018 will require a Data Protection Impact Assessment (DPIA) (Appendix K). DPIAs will be required for the following activities:

- Systematic and extensive profiling or automated decision-making to make significant decisions about people.
- Processing of special category data or criminal offence data on a large scale.
- Systematic monitoring a publicly accessible place on a large scale.
- Use of new technologies.

- Use of profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- Profiling on a large scale.
- Processing of biometric or genetic data.
- Combining, comparing or matching data from multiple sources.
- Processing of personal data without providing a privacy notice directly to the individual.
- Processing personal data in a way which involves tracking individuals' online or offline location or behaviour.
- Processing children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- Processing of personal data which could result in a risk of physical harm in the event of a security breach.

DPIAs may be undertaken in the following circumstances:

- Evaluation or scoring.
- Automated decision-making with significant effects.
- Systematic processing of sensitive data or data of a highly personal nature.
- Processing on a large scale.
- Processing of data concerning vulnerable data subjects.
- Innovative technological or organisational solutions.
- Processing involving preventing data subjects from exercising a right or using a service or contract.

A DPIA (Appendix K) is a process to systematically analyse processing and help to identify and minimise data protection risks. It:

- describe the processing and the purposes
- assess necessity and proportionality
- identifies and assess risks to individuals
- identifies any measures to mitigate those risks and protect the data.

7. Data Protection Officer

As a public authority, the school is obliged to appoint a Data Protection Officer (DPO). The school's DPO is the Business Manager, Kate Davison.

The DPO's tasks specified under the GDPR are to:

- inform and advise the Governing Body and staff about the school's obligations to comply with the GDPR and other data protection laws.
- monitor compliance with the GDPR and other data protection laws.
- create / implement data protection polices, including managing internal data protection activities.
- raise awareness of data protection issues and train staff.
- conduct internal audits.
- advise on, and to monitor, data protection impact assessments.
- cooperate with the supervisory authority.
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

The Governing Body and Headteacher must:

- involve the DPO, closely and in a timely manner, in all data protection matters.

- ensure the DPO reports to the highest management level i.e. the Headteacher.
- support the DPO to operate independently and not dismissed or penalise them for performing their tasks.
- provide adequate resources (sufficient time, financial, infrastructure, and, where appropriate, staff) to enable the DPO to meet their GDPR obligations, and to maintain their expert level of knowledge.
- give the DPO appropriate access to personal data and processing activities.
- give the DPO appropriate access to other services within the school so that they can receive essential support, input or information.
- seek the advice of the DPO when carrying out a DPIA.
- record the details of the DPO as part of your records of processing activities.

It should be noted that the DPO is not personally liable for data protection compliance. As the controller or processor it remains an organisational responsibility to comply with the GDPR.

8. Transferring Data Out of the EU

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. The school does not itself transfer information outside of the EU unless this is specifically requested by a data subject e.g. a student transferring to a school outside of the EU.

Third party processors are expected to confirm that they will not send school data outside of the EU.

9. Personal Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Personal data breaches can include:

- access by an unauthorised third party.
- deliberate or accidental action (or inaction) by a controller or processor.
- sending personal data to an incorrect recipient.
- computing devices containing personal data being lost or stolen.
- alteration of personal data without permission.
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is:

- lost,
- destroyed,
- corrupted or disclosed
- if someone accesses the data or passes it on without proper authorisation
- if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

The GDPR makes clear that when a security incident takes place, the school has an obligation to quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including

informing the Information Commissioner if required. If there is a requirement to inform the Information Commissioner, this will be done so within 72 hours of the school becoming aware of the breach occurring.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR requires the school to inform those concerned directly and without undue delay. Individuals will be told in clear and plain language:

- the nature of the personal data breach.
- the name and contact details of the Data Protection Officer.
- a description of the likely consequences of the personal data breach.
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach.
- Details of the measures taken to mitigate any possible adverse effects.

9.1 Breach Procedure

When a personal data breach occurs, the school will work quickly to establish the likelihood and severity of the resulting risk to people's rights and freedoms. The following procedure is in place:

1. Member of staff notifies either the Headteacher or the Data Protection Officer immediately of the breach.
2. If possible, the school will attempt to contain the breach.
3. Immediate investigation will be undertaken and documented on a Data Protection Breach Report form (Appendix L).
4. Individuals affected will be informed if there is a high risk to their rights and freedoms and advised on how to protect themselves from the effects of the breach.
5. A decision will be made as to whether the breach causes a risk to individual rights and freedoms. If it is felt to pose a risk, the Information Commissioner will be informed.
6. The breach will be noted on the Information Asset Register.
7. As part of the investigation the school will consider how systems and procedures can be improved to prevent a reoccurrence. Actions will be implemented.
8. The Headteacher will consider whether a member of staff has acted negligently or in contravention to school data management processes. If so, sanctions will be made in line with the school's Disciplinary Policy.

10. Children's Data

The GDPR significantly increases the protections for children's data. As an educational establishment, the school primarily processes children's data and takes the security and safeguards of this seriously. Children have the same rights over their data as adults, including the right to see data held about them and privacy notices are written to support them understanding this. The nature of the majority of the processing being under a legal obligation or public task means that there is limited scope for the right to erasure.

11. Archiving

It is possible that data will be retained for historical archives in the public interest or anonymised for statistical analysis. The school will put appropriate technical and organisational measures in order to safeguard the rights and freedoms of individuals

Appendix A: Personal Data Rectification Form

Personal Data Rectification Form

Name:		**Date:**	
Relationship to school:		**Phone no:**	

We make every effort to ensure the personal data that we hold is correct and appreciate your support in making any correction needed. Where there are errors which have been shared with a third party, we will contact them to allow them to correct their records.

In the vast majority of cases the correction will be made quickly and easily. Where we believe we have strong evidence that the data we hold is right, we may not alter the data we hold. Where this is the case, we will contact you and explain the reasons for this.

Please give details of the personal data that you believe to be incorrect including where you have seen this.

Please clearly give the correct version of the data or explain what you feel we need to do to correct the data held.

I confirm that the adjustments I am requesting are correct to the best of my knowledge.					
Signature:		**Print name:**		**Date:**	

School use only	**Request granted?**	**Change made?**	**Third parties notified?**	**Individual contacted?**

Appendix B: Consent Form

Consent Form

Name:		**Date:**	
Relationship to school / Form:		**Phone no:**	

When giving Royds School consent to process your personal data (based on your consent) the following applies:

- **You have a genuine choice and can say no at any time.**
- **You can ask for more information about what we are doing and why.**
- **You can change your mind.**
- **You or your child will not be disadvantaged in any way due to consent being withdrawn.**

We would like to process the following personal data:	
Details of data and the school's proposed use including any third party sharing activity.	**Individual or parent / carer response or requests**

I confirm that I am satisfied with my / my child's personal data being processed in line with the arrangements specified above.

Signature:		**Print name:**		**Date:**	

	Consent given?	**Recorded?**	**Review Date**
School use only			

Appendix C: Withdrawal of Consent Form

Withdrawal of Consent Form

Name:		**Date:**	
Relationship to school or form:		**Phone no:**	

When giving Royds School consent to process your personal data (based on your consent) the following applies:

- **You have a genuine choice and can say no at any time.**
- **You can ask for more information about what we are doing and why.**
- **You can change your mind.**
- **You or your child will not be disadvantaged in any way due to consent being withdrawn.**

Please give details of the processing activity that you have previously consented to and would now like to withdraw consent for.

I confirm that I am withdrawing my consent for the above processing activity.					
Signature:		**Print name:**		**Date:**	

	Request granted?	**Change made?**	**Third parties notified?**	**Individual contacted?**
School use only				

Appendix D: Legitimate Interest Assessment

Legitimate Interest Assessment

Name:		Date:	

Proposed processing activity

Purpose test: are we pursuing a legitimate interest?	
Why do we want to process the data – what are we trying to achieve? Who benefits from the processing? In what way? Are there any wider public benefits to the processing?	How important are those benefits? What would the impact be if we couldn't go ahead? Would our use of the data be unethical or unlawful in any way?

Necessity test: is processing necessary for that purpose?
Does this processing actually help to further that interest? **Is it a reasonable way to go about it?** **Is there another less intrusive way to achieve the same result?**

Balancing test: do the individual's interests override the legitimate interest?	
What is the nature of our relationship with the individual? **Is any of the data particularly sensitive or private?** **Would people expect us to use their data in this way?** **Are we happy to explain it to them?** **Are some people likely to object or find it intrusive?**	**What is the possible impact on the individual?** **How big an impact might it have on them?** **Are we processing children's data?** **Are any of the individuals vulnerable in any other way?** **Can we adopt any safeguards to minimise the impact?** **Can we offer an opt-out?**

Conclusion including processing arrangements and controls

DPO Signature:		**Print name:**		**Date:**	
HT Signature:		**Print name:**		**Date:**	

Appendix E: Subject Access Request Form

Subject Access Request Form

You are entitled to submit a Subject Access Request (SAR) form if you want us to supply you with a copy of any personal data we hold about you. You are entitled to receive this information under the EU General Data Protection Regulation (GDPR).

We will also provide you with information about any processing of your personal data that is being carried out, the retention periods which apply to your personal data, and any rights to rectification, erasure, or restriction of processing that may exist.

We will do our best to respond promptly and in any event within one month of the latest of the following:

- Our receipt of your written request; or
- Our receipt of any further information we may ask you to provide to enable us to comply with your request.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request. You are not obliged to complete this form to make a request, but doing so will make it easier for us to process your request quickly.

1. Details of the person requesting information			
Name:		**Address:**	
Phone number:			
Email address:			

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one of both of the following:

1. Proof of Identity: Passport, photo driving licence, national identity card, birth certificate.
2. Proof of Address: Utility bill, bank statement, credit card statement (no more than 3 months old); current driving licence; current TV licence; local authority tax bill, HMRC tax document (no more than 1 year old).

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request

2. The data subject	
Yes: I am the data subject. I enclose proof of my identity. (Go to section three)	
No: I am acting on behalf of the data subject. I have enclosed the data subject's written authority and proof of the data subject's identity and my own identity.	

Data subject's details			
Name:		**Address:**	
Phone number:			
Form / Role:			

3. Information sought
Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require.
Please note that if the information you request reveals details directly or indirectly about another person we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision. While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, in accordance with Article 12 of the GDPR to charge a fee or refuse the request if it is considered to be "manifestly unfounded or excessive". However we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

4. Information about the collection and processing of data	
If you want information about any of the following, please tick the boxes:	
Why we are processing your personal data	
To whom your personal data are disclosed	
The source of your personal data	

5. Disclosure of CCTV images			
If the information you seek is in the form of video images captured by our CCTV security cameras, would you be satisfied with viewing these images?			
Yes		No	
Please note that it may not always be possible to show you CCTV recordings for example if a person identifiable in the footage has not consented to this. Where issues such as this take place, we will endeavour to share as much as we can in a way that meets your needs.			

6. Declaration					
I confirm that I have read and understood the terms of this subject access form and certify that the information given in this application Royds School is true. I understand that it is necessary for Royds School to confirm my / the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.					
Signature:		**Print name:**		**Date:**	

School use only	
Date of receipt	
Required response date	
Staff member responsible	
Date the information was provided	

Other notes

Appendix F: Erasure of Personal Data Request Form

Erasure of Personal Data Request Form

Name:		**Date:**	
Relationship to school or form:		**Phone no:**	

GDPR gives individuals have the right to have personal data erased in certain circumstances. This right applies when certain criteria apply. Please indicate which criteria you wish to exercise the right to erasure under		
A	The personal data is no longer necessary for the purpose which it was originally collected or processed.	
B	Royds School is relying on consent as the lawful basis for holding the data, and I / my child has withdrawn their consent	
C	The personal data for direct marketing purposes and I / my child objects to that processing	
D	Royds School is relying on legitimate interests as the basis for processing, I / my child objects to the processing of the data	
E	Royds School processed personal data unlawfully	
F	Royds School must erase my data to comply with a legal obligation	
G	Royds School processed the personal data to offer information society services to a child.	

Please give details of the of the personal data you are requesting is erased and where you would like it to be erased from. Please provide any additional evidence to support your request.

I confirm that I am requesting erasure of the above personal data					
Signature:		**Print name:**		**Date:**	

School use only	Request granted?	Change made?	Third parties notified?	Individual contacted?

Appendix G: Request to Restrict Processing Form

Request to Restrict Processing Form

Name:		**Date:**	
Relationship to school or form:		**Phone no:**	

GDPR gives individuals have the right to have personal data restricted in certain circumstances. This right applies when certain criteria apply. Please indicate which criteria you wish to exercise the right to erasure under		
A	I disputes the accuracy of their personal data and want you to verify the accuracy of the data	
B	The data has been unlawfully processed but I don't want it to be erased	
C	Royds School no longer need the personal data but the I want you to keep it in order to establish, exercise or defend a legal claim	
D	I objected to you processing my data under Article 21(1)	

Please give details of the of the personal data you are requesting is restricted and where you whether you would like it to be temporarily or permanently restricted. Please provide any additional evidence to support your request.

I confirm that I am requesting restriction of the above personal data					
Signature:		**Print name:**		**Date:**	

School use only	**Request granted?**	**Restriction arrangements?**	**Third parties notified?**	**Individual contacted?**

Appendix H: Data Portability Request Form

Data Portability Request Form

Name:		**Date:**	
Relationship to school:		**Phone no:**	

Please give details of the personal data that you would like to receive or to be transferred to a third party and the format you would prefer to receive it in

If you would like it to be transferred to another establishment, please give a contact name and address below

I confirm that I would like to receive the above data and I consent to Royds School sharing this with the above named third party					
Signature:		**Print name:**		**Date:**	

	Request granted?	**Information sent**	**Third parties informed**	**Individual contacted?**
School use only				

Appendix I: Objection to Personal Data Processing Form

Objection to Personal Data Processing Form

Name:		**Date:**	
Relationship to school or form:		**Phone no:**	

GDPR gives individuals have the right to object to personal data being processed in certain circumstances. This right applies when certain criteria apply. Please indicate which criteria you wish to exercise the right to erasure under		
A	I processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority	
B	Direct marketing (including profiling)	
C	Processing for purposes of scientific/historical research and statistics	

Please give details of the of the personal data you are requesting is restricted and where you whether you would like it to be temporarily or permanently restricted. Please provide any additional evidence to support your request.

I confirm that I am objecting to the processing of the above personal data					
Signature:		**Print name:**		**Date:**	

School use only	**Request granted?**	**Actions**	**Third parties notified?**	**Individual contacted?**

Appendix J: Third Party Processor Contract

Third Party Processor Contract

Royds School, the data controller, is entering into the following contract:			
Data processor:		**Agreement date:**	

The subject matter and duration of the processing is as follows:

The nature and processing of the processing is as follows:

The types of personal data and categories of data subject are as follows:	
Types of personal data	**Categories of data subject**

The obligations and rights of the controller are as follows:

The following terms are compulsory as specified by the Information Commissioner:	
1	The processor must only act on the written instructions of the controller, unless required by law to act without such instructions.
2	The processor must ensure that people processing the data are subject to a duty of confidence.
3	The processor must take appropriate measures to ensure the security of processing.
4	The processor must only engage a sub-processor with the prior consent of the data controller and a written contract.
5	The processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR.
6	The processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments.
7	The processor must delete or return all personal data to the controller as requested at the end of the contract.
8	The processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

As a matter of good practice as a data controller, our contract include the following terms recommended by the Information Commissioner:	
1	Nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR.
2	Unless stated within this contract, no indemnity has been agreed.
3	The processor must comply with its own obligations as a processor under the GDPR.

Signed on behalf of:					
Data Controller Royds School					
Signature:		Print name:		Date:	
Data Processor: XXX					
Signature:		Print name:		Date:	

Appendix K: Data Protection Impact Assessment

Data Protection Impact Assessment

Name:		Date:	

Does the processing meet any of the following criteria?		
A DPIA must be carried out if any of criteria A-L are met. It would be good practice to continue with the DPIA if any of criteria M-T are met. The DPIA can still be completed if no criteria are met		
A	Systematic and extensive profiling or automated decision-making to make significant decisions about people.	
B	Process special category data or criminal offence data on a large scale.	
C	Systematically monitor a publicly accessible place on a large scale.	
D	Use new technologies	
E	Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit	
F	Carry out profiling on a large scale.	
G	Process biometric or genetic data.	
H	Combine, compare or match data from multiple sources.	
I	Process personal data without providing a privacy notice directly to the individual.	
J	Process personal data in a way which involves tracking individuals' online or offline location or behaviour.	
K	Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.	
L	Process personal data which could result in a risk of physical harm in the event of a security breach.	
M	Evaluation or scoring.	
N	Automated decision-making with significant effects.	
O	Systematic processing of sensitive data or data of a highly personal nature.	
P	Processing on a large scale.	
Q	Processing of data concerning vulnerable data subjects.	
R	Innovative technological or organisational solutions.	
S	Processing involving preventing data subjects from exercising a right or using a service or contract.	

Details of the proposed activity	
Nature of the processing	
Scope of the processing	
Purpose of the processing	
Categories of individuals and data	
Third parties involved	
Technology involved	

If a decision is made not to proceed with the DPIA, please document the reasons below.

Stakeholder consultation arrangements

Explain how processing is necessary for and proportionate to the intended purposes.

Describe the arrangements to ensure data protection compliance.

Risks of processing to individual rights and proposed safeguards		
	Risks including likelihood and severity	Safeguards
Right to be informed		
Right of access		
Right to rectification		
Right to erasures		
Right to restrict processing		
Right to data portability		
Right to object		
Rights in relation to automated processing		

Conclusion including processing arrangements and controls. Include any difference of opinion with the outcome of stakeholder consultation

Data Protection Officer comments

DPO Signature:		**Print name:**		**Date:**	
HT Signature:		**Print name:**		**Date:**	

Appendix L: Data Protection Breach Report Form

Data Protection Breach Report Form

Staff Reporting Breach Name:		**Date of Breach:**	
Investigator Name:		**Time of Breach**	

Summary of the incident

Please identify the type(s) of breach:		
A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.		
A	Access by an unauthorised third party.	
B	Deliberate or accidental action (or inaction) by a controller or processor.	
C	Sending personal data to an incorrect recipient.	
D	Computing devices containing personal data being lost or stolen.	
E	Alteration of personal data without permission.	
F	Loss of availability of personal data.	
G	Other loss of personal data.	
H	Destruction of personal data.	
I	Sharing personal data without proper authorisation.	
J	Access to data without appropriate authorisation.	
K	Other.	

Details of the breach	
Circumstances leading to the breach	
Data lost / compromised. Include categories and number of individuals and records.	
Security measures for the data lost	
Actions taken by the source of the breach	
School actions following the breach	

Describe how the affected individuals have been informed and the advice given to protect themselves following the incident.

Explain whether the data breach lead to a risk to the rights and freedoms of the individuals concerned

Explain the potential consequences of the data breach

Does the school feel the breach meets the criteria for informing the Information Commissioner?
If yes, please document the response of the Information Commissioner.
If no, please document the reasons for this decision.

Lessons learned, including how systems and procedures can be improved to ensure a similar breach does not occur again.

Data Protection Officer comments

DPO Signature:		**Print name:**		**Date:**	
HT Signature:		**Print name:**		**Date:**	

Royds