St Robert Southwell Catholic Primary School

Aiming for Excellence - Being the Best We Can Be

Data Protection Policy

GDPR

Approved & adopted by Governors: July 2020
Last review: May 2021
Next Review: May 2022

Following Jesus' footsteps and inspired by St. Robert Southwell we work hard, aim high and treat everyone with honesty and gentleness

St Robert Southwell Catholic Primary School

Aiming for Excellence - Being the Best We Can Be

Data Protection Policy

This policy complies with the requirements set out in the GDPR, which came into effect on 25th May 2018. The UK government have confirmed that the decision to leave the EU will not affect the commencement of GDPR.

Contents

St Robert Southwell Catholic Primary School

Aiming for Excellence - Being the Best We Can Be

MISSION STATEMENT

Our mission is to create an educating Christian community which reflects the values of the Gospel within the traditions of the Roman Catholic Church;

- a community which will develop the whole person
- a community which works closely with parents and parish
- a community which values each child as a unique individual with particular gifts and needs
- a forward-looking community which serves its members and the wider society
- a community in which we will lead those in our care to grow in their faith whilst benefiting from an enriching education.
-

Wellbeing & Mental Health

To support everyone's wellbeing and mental health, so that they can be the best they can be, are happy together, resilient, ready to learn and succeed

- Empowering everyone in the community to be emotionally literate
- Enabling stakeholders to develop strategies to manage their emotional wellbeing and mental health.

1 Policy statement

1.1 Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as a School we will collect, store and **process personal data** about our pupils, **workforce**, parents and others. This makes us a **data controller** in relation to that **personal data**.

1.2 We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

1.3 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

1.4 All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

1.5 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 **GDPR**.

1.6 Everyone managing and handling information, particularly **personal** information needs to understand their responsibilities in complying with the legislation and codes of practice. It is the personal responsibility of:-

- All employees of the school
- All employees and agents of other organisations who directly or indirectly support or are procured by the School, including all temporary and agency staff directly or indirectly employed by the School.
- Those engaged on interim contractual arrangements or agency contracts working on behalf of the School.
- Supplies and **Data Processors** of the School

1.7 The governing body has overall responsibility for ensuring that the School complies with all relevant **data protection** obligations. The headteacher acts as the representative of the governing body on a day to day basis.

1.8 The School has a clear commitment to ensuring that all staff have access to appropriate training or guidance. Staff managing and handling **personal data** and other information are adequately trained with regard to the requirements of this an all other information governance policy.

1.9 Organisational methods for keeping data secure are imperative and St. Robert Southwell Catholic Primary school believes that it is good practice to keep clear practical policies, backed up by written procedures.

2 About this policy

2.1 The types of **personal data** that we may be required to handle include information about pupils, parents/carers, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation ('**GDPR**'), the Data Protection Act 2018, and other regulations (together '**Data Protection Legislation**'). The Freedom of Information Act 2000, The Education (Pupil information) England Regulations 2005 (amended 2016), The Freedom of Information and Data Protection (appropriate limit and fees) regulations 2004, The School Standards and Framework Act 1998. This Policy also has regard to the following guidance – ICO (2018) Guide to GDPR.

2.2 This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

2.5 The School has privacy notices in place for pupils, parents/carers, staff & workforce and Governors & volunteers. These Privacy Notices ensure that individuals are aware of how the School use their personal information. These are supported in other ways to tell individuals how their information will be used e.g. verbally, forms and other information.

3 Definition of data protection terms

3.1 All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in the Annex to this policy.

4 Data Protection Officer

4.1 As a School we are required to appoint a Data Protection Officer ("DPO"). Our DPO is Deepti Bal and they can be contacted at dpo.bal@bsp.london

4.2 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

4.3 The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

5 Data protection principles

5.1 Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

5.1.1 **Processed** fairly and lawfully and transparently in relation to the **data subject**;

5.1.2 **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;

5.1.3 Adequate, relevant and not excessive for the purpose;

5.1.4 Accurate and up to date;

5.1.5 Not kept for any longer than is necessary for the purpose; and

5.1.6 **Processed** securely using appropriate technical and organisational measures.

5.2 **Personal Data** must also:

5.2.1 be **processed** in line with **data subjects'** rights;

5.2.2 not be transferred to people or organisations situated in other countries without adequate protection.

5.3 We will comply with these principles in relation to any **processing** of **personal data** by the School

6 Fair and lawful processing

6.1 Data Protection Legislation is not intended to prevent the **processing** of **personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the **data subject**.

6.2 For **personal data** to be **processed** fairly, **data subjects** must be made aware:

6.2.1 that the **personal data** is being **processed**;

6.2.2 why the **personal data** is being **processed**;

6.2.3 what the lawful basis is for that **processing** (see below);

6.2.4 whether the **personal data** will be shared, and if so with whom;

6.2.5 the period for which the **personal data** will be held;

6.2.6 the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and

6.2.7 the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

6.3 We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered and will ensure that we have a lawful basis for any **processing**.

6.4 For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally **process personal data** under the following legal grounds:

6.4.1 where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;

6.4.2 where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g the Education Act 2011);

6.4.3 where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest; and

6.4.4 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data.**

6.5 When **special category personal data** is being processed then an additional legal ground must apply to that processing. We will normally only **process special category personal data** under following legal grounds:

6.5.1 where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;

6.5.2 where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;

6.5.3 where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and

6.5.4 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **special category personal data**.

6.6 We will inform **data subjects** of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

6.7 If any **data user** is in doubt as to whether they can use any **personal data** for any purpose then they must contact the DPO before doing so.

Vital Interests

6.8 There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not in a position to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances.

In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

6.9 Where none of the other bases for **processing** set out above apply then the school must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.

6.10 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

6.11 When pupils and or our Workforce join the School a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

6.12 In relation to all pupils under the age of 12 years old we will seek consent from an individual with parental responsibility for that pupil.

6.13 If consent is required for any other **processing** of **personal data** of any **data subject,** then the form of this consent must:

6.13.1 Inform the **data subject** of exactly what we intend to do with their **personal data**;

6.13.2 Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and

6.13.3 Inform the **data subject** of how they can withdraw their consent.

6.14 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent.

6.15 The DPO must always be consulted in relation to any consent form before consent is obtained.

6.16 A record must always be kept of any consent, including how it was obtained and when.

7 Processing for limited purposes

7.1 In the course of our activities as a School we may collect and **process** the **personal data** set out in our Schedule of Processing Activities. This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our **workforce**).

7.2 We will only **process personal data** for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

8 Notifying data subjects

8.1 If we collect **personal data** directly from **data subjects**, we will inform them about:

8.1.1 our identity and contact details as **Data Controller** and those of the DPO;

8.1.2 the purpose or purposes and legal basis for which we intend to **process** that **personal data**;

8.1.3 the types of third parties, if any, with which we will share or to which we will disclose that **personal data**;

8.1.4 whether the **personal data** will be transferred outside the European Economic Area ('**EEA**') and if so the safeguards in place;

8.1.5 the period for which their **personal data** will be stored, by reference to our Retention and Destruction Policy;

8.1.6 the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making; and

8.1.7 the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

8.2 Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter, informing them of where the **personal data** was obtained from.

9 Adequate, relevant and non-excessive processing

9.1 We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

10 Accurate data

10.1 We will ensure that **personal data** we hold is accurate and kept up to date.

10.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

10.3 **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

11 Timely processing

11.1 We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required. Please refer to the School's Retention policy for how the School retains and removes data.

12 Processing in line with data subject's rights

12.1 We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

12.1.1 request access to any **personal data** we hold about them;

12.1.2 object to the **processing** of their **personal data**, including the right to object to direct marketing;

12.1.3 have inaccurate or incomplete **personal data** about them rectified;

12.1.4 restrict **processing** of their **personal data**;

12.1.5 have **personal data** we hold about them erased

12.1.6 have their **personal data** transferred; and

12.1.7 object to the making of decisions about them by automated means.

The Right of Access to Personal Data

12.2 **Data subjects** may request access to all **personal data** we hold about them. Such requests will be considered in line with the School's Subject Access Request Procedure – also see CCTV policy.

The Right to Object

12.3 In certain circumstances **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

12.4 An objection to **processing** does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the **data subject**.

12.5 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

12.6 In respect of direct marketing any objection to **processing** must be complied with.

12.7 The School is not however obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings or a matter of Safeguarding/Child protection.

The Right to Rectification

12.8 If a **data subject** informs the School that **personal data** held about them by the School is inaccurate or incomplete, then we will consider that request and provide a response within one month.

12.9 If we consider the issue to be too complex to resolve within that period, then we may extend the response period by a further two months. If this is necessary, then we will inform the **data subject** within one month of their request that this is the case.

12.10 We may determine that any changes proposed by the **data subject** should not be made. If this is the case, then we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

12.11 **Data subjects** have a right to "block" or suppress the **processing** of **personal data**. This means that the School can continue to hold the **personal data** but not do anything else with it.

12.12 The School must restrict the **processing** of **personal data**:

12.12.1 Where it is in the process of considering a request for **personal data** to be rectified (see above);

12.12.2 Where the School is in the process of considering an objection to processing by a **data subject**;

12.12.3 Where the **processing** is unlawful but the **data subject** has asked the School not to delete the **personal data**; and

12.12.4 Where the School no longer needs the **personal data** but the **data subject** has asked the School not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the School.

12.13 If the School has shared the relevant **personal data** with any other organisation, then we will contact those organisations to inform them of any restriction unless this proves impossible or involves a disproportionate effort.

12.14 The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

12.15 **Data subjects** have a right to have **personal data** about them held by the School erased only in the following circumstances:

12.15.1 Where the **personal data** is no longer necessary for the purpose for which it was originally collected;

12.15.2 When a **data subject** withdraws consent – which will apply only where the School is relying on the individual's consent to the **processing** in the first place;

12.15.3 When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object;

12.15.4 Where the **processing** of the **personal data** is otherwise unlawful;

12.15.5 When it is necessary to erase the **personal data** to comply with a legal obligation; and

12.15.6 If the School offers information society services to a pupil and consent is withdrawn in respect of that pupil in relation to those services.

12.16 The School is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:

12.16.1 To exercise the right of freedom of expression or information;

12.16.2 To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;

12.16.3 For public health purposes in the public interest;

12.16.4 For archiving purposes in the public interest, research or statistical purposes; or

12.16.5 In relation to a legal claim.

12.17 If the School has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

12.18 The DPO must be consulted in relation to requests under this right.

Right to Data Portability

12.19 In limited circumstances a **data subject** has a right to receive their **personal data** in a machine-readable format, and to have this transferred to other organisation.

12.20 If such a request is made, then the DPO must be consulted.

13 Data security

13.1 We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**.

13.2 We will put in place procedures and technologies to maintain the security of all **personal data** from the point of collection to the point of destruction.

13.3 Security procedures include:

13.3.1 **Entry control.** Access control system in place. Staff are issued with contactless ID card & badge. Access is granted to specific areas only. Cards can be issued to visitors or temporary staff, but access will be restricted to general populated areas only. This system also has the ability to "lockdown" the school in the case of an emergency.

13.3.2 **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential). If necessary, items can be stored in a safe with restricted access.

13.3.3 **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.

13.3.4 **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

13.3.5 **Network security.** Anti-virus and anti-malware software – a review of protection on a regular basis is carried out to ensure protection is still fit for purpose.

13.3.6 **Encryption.** Digital data is coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks need serious consideration as they are easy to lose and their use should be avoided. They must not be used to hold personal information unless they are password protected and fully encrypted.

All electronic devices are password protected to protect the information on the device in case of theft.

Members of staff are provided with their own secure login and password for use on the School's computer and CPOMS system. Specified members of staff also have secure login and passwords to certain software packages, such as the parent communication app, SIMS and Scopay.

13.3.7 **Ensuring authorised access.** Only people who have a need to know the personal data are authorised to access it. 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.

13.3.8 **Confidentiality & Clear desk policy.** Adhering to confidentiality principles. Confidential paper records will not be left unattended or in clear view anywhere with general access. A clear desk policy is the best way to avoid unauthorised access to physical records which contain sensitive or personal information.

13.3.9 **Working away from the school premises – paper documents** When 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.

13.3.10 **Working away from the school premises – electronic working.** Staff sign an ICT Use Policy and Off-Site Equipment Register & Agreement, agreeing to use the provision for work purposes and reasonable personal use. The equipment remains the property of the School and will be returned when employment ceases or requested by the School. The School's policies, as would be required if working on the school premises, e.g. Internet/email usage, Data Protection, still apply.

A remote access solution allows access to any files, databases or information systems on the network whilst the member of staff or student is not physically located in the school. It should have strong security controls put in place and regular reviews to ensure that it is still secure.

Restrictions should be set if necessary, to prevent information or records being downloaded, transferred or printed whilst the user is offsite. Devices connecting to any remote access system should be considered as part of the network and all appropriate security measures should be taken to protect the network and all systems from possible attacks from that device or any other source.

13.3.11 **Document printing.** Documents containing **personal data** must be collected immediately from printers and not left on photocopiers – use the secure print option when printing.

13.3.12 **Sharing data.** All staff members will ensure they are allowed to share it, that adequate security is in place to protect it and who will receive the data has been outlined in a privacy notice.

13.3.13 Emails containing sensitive or confidential information are password protected if there are unsecure servers between the sender and recipient. However, it would be best practice to password protect all sensitive attachments internally and externally.

13.3.14 Telephone calls and meetings to be held in private areas to avoid sensitive information being overheard.

13.3.15 No documents containing personal information to be pinned to noticeboards in the classroom. No documents containing personal information to be pinned to noticeboards in offices or staffrooms if accessible by visitors, pupils, parents or unauthorised personnel.

13.3.16 Staff should be particularly alert to the need to shred trip packs upon return to school, particularly since they will contain particularly sensitive health and behavioural data of the pupils concerned.

13.4 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

14 Data Protection Impact Assessments

14.1 The School takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

14.2 In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.

14.3 The School will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.

14.4 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

15 Disclosure and sharing of personal information

15.1 We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, Ofsted, health authorities and professionals, welfare services (Social Services), the Local Authority, Local Authority Designated Officer (LADO) examination bodies, other schools, law enforcement officials such as the police, HMRC, DBS and other organisations where we have a lawful basis for doing so.

15.2 The School will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.

15.3 In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

15.4 Further detail is provided in our Schedule of Processing Activities.

16 **Data Processors**

16.1 We contract with various organisations who provide services to the School including:

- Professional advisors such as lawyers and consultants
- Support services - including insurance, HR support, IT support, information security, parent communication and payment software providers, pensions and payroll
- Providers of learning software
- School catering company
- Prospective Employers
- Training providers
- Occupational Health
- Recruitment and supply agencies
- The Diocese of Westminster

16.2 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

16.3 **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the School. The School will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

16.4 Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.

17 **Images and Videos**

17.1 Parents and others attending School events are prohibited to take photographs or recordings of the event i.e. play, assembly or display. Organised photographs as directed by the School may be allowed to take place at the end of the event at the discretion of the Headteacher. Recordings and pictures may be taken by the school for parents/carers to purchase to add to School funds.

17.2 The School does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the School to prevent.

17.3 The School asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

17.4 As a School we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils on our website or our Twitter page, within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent from parents/carers where appropriate, before allowing the use of images or videos of pupils for such purposes.

17.5 Whenever a pupil begins their attendance at the School, their parent will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

18 CCTV

18.1 The School operates a CCTV system. Please refer to the School CCTV Policy.

19 Related Policies

- Records Management & Retention Policy
- Information Security Policy
- CCTV Policy
- Data Breach Policy
- Subject Access Request (SAR) Policy
- Freedom of information Policy & ICO Publication Scheme

20 School archive

The School archive is maintained as a resource to help inspire and equip current staff and pupils to understand and appreciate issues of identity, belonging and shared heritage; to prompt memories of school-life among many generations of former pupils; and to serve as a research resource for all interested in the history of the School and the community it serves. A small percentage of the School's records will be selected for permanent preservation as part of the School's archives and for historical research.

21 Changes to this policy

We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

We will monitor and review how our policy and procedures are working in practice to reduce the risks posed to the School.

ANNEX

DEFINITIONS

Term	Definition
Data	is information, which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our workforce (including Governers and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Workforce	Includes, any individual employed by the School such as staff and those who volunteer in any capacity including Governors, parent helpers and placement volunteers