








Our vision is ***to enable children to become lifelong learners by creating a safe and inclusive learning environment that nurtures individuality and enhances potential***

Our values:

-  ***We're imaginative*** - we're creative thinkers and doers
-  ***We're curious*** - we encourage inquisitiveness and risk taking
-  ***We're proud*** - we take pride in our school and want everyone to succeed
-  ***We're courageous*** - we understand that we learn from our mistakes
-  ***We're original*** – we celebrate difference

INTERNAL DATA SECURITY

Schools and academies are legally required to be able to demonstrate compliance with the General Data Protection Regulation (GDPR).

This policy should be read in conjunction with the following:

- The privacy notices applicable at the school or academy.
- E-safety.
- Freedom of information – publication scheme.
- ICT and use of the internet and intranet by staff.
- Management and retention of records.
- Personnel record keeping.
- Risk management procedure.
- Staff email.
- Use of personally owned devices by staff.

The legislation which applies is the General Data Protection Regulation 2018 (GDPR), the Data Protection Act 2018 and the Protection of Freedoms Act 2012. Other documents which may assist include:

- Information Commissioner's Office (ICO) – What is personal data? – A quick reference guide <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data>.
- ICO: GDPR at a glance <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security>.
- ICO: Report on the data protection guidance we gave to schools in 2012 <https://ico.org.uk/media/action-weve-taken/self-assessments/2790/report-dp-guidance-for-schools.pdf>.
- Data Protection Toolkit for schools: www.gov.uk/government/publications/data-protection-toolkit-for-schools

INTERNAL DATA SECURITY POLICY

Background

Under the Data Protection Act 1998 it was the responsibility of each school to register as a data controller on the data protection register held by the Information Commissioner's Office (ICO). The General Data Protection Regulation (GDPR) changed this position with data controllers no longer having to register but still having to pay a fee to fund the work of the ICO under the Data Protection (Charges and Information) Regulations 2018, which came into force on 25 May 2018. The fee is payable unless the organisation is exempt.

Further information regarding the fee process can be found at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-fee>.

Introduction

It is the requirement of all organisations to demonstrate compliance with the GDPR and the Data Protection Act 2018.

Schools are data rich and the introduction of electronic storage and transmission of data has created additional potential for the loss, destruction or mismanagement of data.

While the focus of this policy is primarily on personal data, as defined below, equally there may be instances where data relates to the school or academy and is commercially sensitive and therefore ought to be protected from misuse and data breaches.

The school, in processing personal data, must ensure that all its staff are aware of the requirements of the GDPR and their respective obligations to protect the confidentiality and integrity of personal data. Failing to do so can result in significant financial penalties and sanctions to the school and possibly to any individual who breaches the requirements of the GDPR.

The school has a data protection officer (DPO) who will keep the school up-to-date with current legislation and guidance. The DPO will be a first point of contact for any issues regarding GDPR compliance. Advice should be sought from the DPO regarding school policies and the day-to-day management and use of personal data.

It is important to stress that this policy applies to all forms of data, including personal data, regardless of whether it is held on paper or in electronic format.

What is personal data and what does processing mean?

Personal information is any information that relates to you and can be used directly or indirectly to identify a living individual.

Personal information and processing are defined as follows:

- **Data** means information in whatever form (including, without limitation, in written, oral, visual or electronic form or on any magnetic or optical disk or memory and wherever located) relating to the business, products, affairs and finances of the school for the time being confidential to the school and trade secrets including, without limitation, technical data and know-how relating to

the business of the school or any of its suppliers, clients, customers, agents, distributors, shareholders or management, including personal data.

- **Personal data** means any information relating to an identified or identifiable natural person (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.
- **Special categories of personal data** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric/genetic data.
- **Processing or to process** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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.

Scope

It is the responsibility of all members of the school community to take care when processing data to avoid data breaches and/or falling foul of the legislative requirements of the GDPR and the Data Protection Act 2018.

A data breach can happen if:

- Data is lost.
- Data is accessed without authorisation or without proper legal right/permission to do so.
- Data is disclosed or acquired without authorisation or without proper legal right/permission to do so.
- Data is destroyed unlawfully.
- Data is not maintained securely.
- Confidentiality of data is not maintained.
- Protections put in place to maintain data including technical, organisational and administrative safeguards are ignored, undermined and not adhered to.

Any loss of data or personal data can have serious effects for individuals and/or institutions concerned. It can bring the school into disrepute and may well result in disciplinary action and/or prosecution/enforcement proceedings.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in current relevant data legislation and regulations.

The loss of personal data by organisations and individuals over the last few years has made this a relevant and high profile issue for schools and all organisations. It is important that the school has a clear and well understood personal data policy because:

- No school or individual would want to be the cause of any loss of data, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
- The school will want to avoid the criticism and negative publicity that could be generated by any loss of data.
- The school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.

Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations.

Legislation covering the safe handling of this data was, until 25 May 2018, addressed by the UK Data Protection Act 1998. Following a number of losses of sensitive data, a report was published by the Cabinet Office in June 2008 regarding Data Handling Procedures in Government. This stipulated the procedures that all departmental and public bodies should follow in order to maintain security of data. Given the personal and sensitive nature of much of the data held in schools, it is critical that such procedures are adopted.

Personal data can be a combination of data items that identifies an individual and provides specific information about them, their families or circumstances.

This can include:

- Personal information about members of the school community – including pupils/students, members of staff, parents and carers eg names, addresses, contact details, legal guardianship, health records, disciplinary records.
- Curricular/academic data eg class lists, pupil/student progress records, reports, references.
- Professional records eg employment history, taxation and national insurance records, appraisal records and references.
- Information that might be disclosed by parents/carers or by other agencies working with families or staff members.

Data breaches

The GDPR requires that we notify the ICO and, in some circumstances, the data subject of any personal data breaches within 72 hours of becoming aware of the breach.

We have put in place protocol to deal with any suspected personal data breach and will notify the appropriate personnel where it is necessary to do so.

If you know or suspect that a data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO and retain all evidence of the suspected breach so that the matter can be properly investigated.

Principles

As the role of management information systems (MIS) continues to develop, colleagues in schools have increasing access to a wide range of sensitive information. The GDPR has introduced a new definition for sensitive information of personal data known as special categories of personal data – this was defined on page 3. Particular care must be taken when processing special categories of personal data.

It is important to ensure that all types of information are managed in a secure way at all times. However, personal data is the most likely form of sensitive data that a school will hold.

The GDPR states that personal data must be processed in accordance with the data protection principles. Staff must adhere to and be committed to these principles as follows:

- We process personal data lawfully, fairly and in a transparent way.
- We collect personal data only for specified, explicit and legitimate purposes.
- We process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- We keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- We keep personal data only for the period necessary for processing.
- We adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, accidental loss, destruction or damage.
- In our privacy notices, we tell individuals the reasons for processing their personal data, how we use such data and the legal basis for processing. We will not process personal data of individuals for reasons other than the stated purpose or purposes.
- Where we process special categories of personal data or criminal records data to perform obligations, this is done in accordance with a policy, or for legal reasons. We will update personal data promptly if an individual advises us that his/her information has changed or is inaccurate.

Failing to adhere to the principles can result in disciplinary action for the individual concerned, as well as penalties and sanctions for the school. Further guidance on how the school and its staff will adhere to the principles is contained below.

Lawfulness and fairness

Under the GDPR, personal data must be processed in a lawful, fair and transparent way.

Members of the school community may only collect, process and share personal data in accordance with that principle and for any specified purposes as contained within the school's privacy notices.

The GDPR restricts processing personal data to specified lawful purposes. This is to ensure that a data subject's privacy rights are always considered and maintained.

At least one of the following legal grounds must exist in order for the processing of personal data to be lawful and GDPR compliant:

- You have consent of the data subject (or their parent/guardian).
- The processing is necessary for the performance of a contract.
- The processing is to meet legal obligations.
- The processing is to protect the vital interests of the data subject.
- The processing is to pursue our legitimate interests (as set out in our privacy notices).
- The processing is in the public interest.

We have documented the legal basis upon which we process the personal data we hold. You must make sure you are aware of this and only process the personal data for the reasons stated and for the basis upon which we have described.

If you are not sure about this or a reason not currently covered by our documentation arises you must speak to the DPO before releasing or processing any data.

Consent

Consent is one of the lawful grounds by which personal data can be processed by the school. Consent must be fully informed and unambiguous meaning that the data subject must be clear as to what they are consenting to and the reasons for it. Particular care must be taken when processing special categories of personal data because a higher threshold is required for such information.

Consent will only apply in some specific circumstances because the other lawful grounds are usually more appropriate when processing the personal data of pupils, parents, guardians and staff.

Consent should be in writing so that it can be evidenced at a later stage. Consent can be withdrawn at any time. Fresh consents must be obtained if the personal data it covers, or the purpose for processing, becomes invalid or incompatible with the new processing requirements.

If you believe that consent is required for you to process certain types of personal data and you do not have it, or you do not believe it is clear and unambiguous, you must obtain it before carrying out the processing. You must speak to the DPO if you are unclear about this requirement or need assistance.

Privacy notices

The school's obligations under the GDPR include providing specific information to data subjects on the information that we collect, retain and generally process. This requirement is to be transparent in the way we process personal data.

Transparency means that we are required to specify the purposes for which we process personal data, how long we may hold the information for and what the data subject's rights are.

We have included this information within the school's privacy notices. You must be familiar with the privacy notices because they contain a lot of information about how the school and therefore how you may process personal data and the reasons why.

Crucially, we are not allowed to process personal data for a purpose that is incompatible with one of the stated purposes in our privacy notices. While we have sought to identify all the purposes for which we process personal data in our privacy notices it may be that the stated purposes have to be extended in certain circumstances. Any issues that arise in relation to this should be referred to the DPO.

If you are unclear about your obligations and duties or require assistance with any of the privacy notices you must speak to the DPO for guidance.

Students deemed to be of a suitable age (usually 13+) are also made aware of the privacy notice, the school's legal obligations to pass on certain information, eg to providers of youth support services, and their rights to request the school to withhold certain information.

Our privacy notices for parents, guardians and pupils are worded incorporating the current DFE template and its circulation is supervised by our DPO.

Accuracy

To comply with the data protection principles we must ensure that personal data is accurate and, where necessary, kept up-to-date.

Where data is not accurate it must either be corrected or deleted straight away.

Staff members are required to check the accuracy of the personal data they process and, when any errors or issues arise, they must take all reasonable steps to resolve them.

If you are unclear as to your obligations to maintain accurate records please contact the DPO.

Retention periods and storage limitation

Personal data in an identifiable form must be kept only for as long as the stated purposes when considering the personal data we process.

This obligation only relates to the data being in an identifiable form, that is a form that allows the identification of the data subject from the personal data. As such, it may be the case that the identifying features of the personal data can be removed after a certain period of time. In other instances, personal data must be confidentially and securely destroyed.

It is important to remember that some data will need to be retained for legal or other compliance reasons. So to comply with this obligation, the school has developed a retention schedule that all staff must adhere to. This stipulates the relevant time frames by which the various categories of personal data can be held, pseudonymised or otherwise destroyed.

Data security measures: integrity and confidentiality

One of the principles of the GDPR is to maintain the integrity and confidentiality of personal data. At the school this principle can also be extended to data generally.

Information security is at the forefront of the GDPR's key requirements. Every aspect of data security must be considered with technological and administrative processes being key to avoiding threats to the security of personal data. Appropriate security measures must be implemented that are appropriate to the risks to the data.

- The school will encrypt any data that is determined to be personal or commercially sensitive in nature. This includes data held on fixed station computers, laptops, portable devices and memory sticks.
- All staff will be trained to understand the need to handle data securely and the responsibilities incumbent on them.
- The school has a clear policy and a procedure for the use of cloud-based storage systems and is aware that data held in remote cloud storage is still required to be protected in line with the GDPR. The school will ensure that it is satisfied with the controls put in place by service providers to protect the data.
- Biometric data complies with the same data protection principles outlined above and also with the Protection of Freedoms Act 2012. We ensure that each parent of a child at the school is notified that we use their child's biometric data as a part of our automated biometric information system. Since September 2013, the written consent of the parents is obtained before the data is taken from all pupils under 18 years of age. We will not process this data if the child under 18 (if deemed competent to understand the issue) refuses or if no parents or only one of two parents have consented in writing. The school provides alternative means of accessing services for those pupils who will not be using an automatic biometric recognition service.
- Staff should *not* copy or remove special categories of personal data or commercially sensitive data from the school or authorised premises unless the media are:
 - Encrypted.
 - Transported securely.
 - Stored in a secure location.
- Sensitive data *should not* be transmitted in unsecured emails (eg pupil names and addresses, performance reviews etc).
- Data transfer should be through secure websites. If this is not available, then the file must be password protected or preferably encrypted before sending via email. The password must be sent by other means, and on no account included in the same email. A record of the email should be kept to identify when, and to whom, the email was sent. (The DfE website contains a useful section – Transferring personal data securely between schools, LAs and the Department (updated March 2014). This provides comprehensive guidance on transferring information. www.gov.uk/government/publications/school-to-school-guides-for-schools-and-local-authorities.)
- Data (pupil records, SEN data, contact details, assessment information) must be automatically backed up, encrypted and stored in a secure place – eg safe/fire safe/remote backup facility.
- All staff computers, including laptops, must be used in accordance with the policy for ICT and use of the internet and intranet by staff.

- When laptops are passed on or re-issued, data will be securely wiped from any hard drive before the next person uses it (not simply deleted). This will be done by the school's ICT technical support staff.
- The school's wireless network (wifi) will be secure at all times.
- Devices that are not the property of the school should only be used in line with our policy on the use of personally owned devices by staff.
- The school will ensure that staff who are responsible for sets of information, such as SEN, medical, vulnerable learners, management data etc know what data is held, who has access to it, how it is retained and how and when it is disposed of.
- Where a member of the school has access to data remotely, the remote access off the school site to any personal data should be over an encrypted connection (eg VPN) protected by a username/ID and password. This MIS information/school data must not be stored on a personal (home) computer.
- Members of staff who are given full, unrestricted access to the school's management information system must access the systems over an encrypted connection. This MIS information/school data must not be stored on a personal (home) computer.
- The school will keep necessary pupil and staff information in accordance with the Information and Records Management Society's (IRMS) guidance and the records retention policy.
- The school will securely delete commercially sensitive or personal data when it is no longer required according to the IRMS's guidance and the records retention policy.

Data should remain confidential and you should not share it with any unauthorised personnel or third parties.

If you fail to adhere to the policies and procedures, disclose the data in circumstances where you are not lawfully permitted to do so or otherwise seek to circumvent the data security measures that are in place, you may face disciplinary proceedings.

Obligations under this policy

The purpose of this policy is to advise all members of staff what is required by the school to ensure that it complies with the GDPR and Data Protection Act 2018 at all times, and to advise all members of staff how to proceed when handling data which needs to be handled securely.

You should contact the DPO if you are unsure about your obligations contained within this policy or are otherwise unsure about your obligations under the GDPR. Examples of where you may want to speak to the DPO include:

- If you are not sure of the lawful basis for which you are processing any personal data.
- If you are not sure of the retention period for holding a particular piece of personal data or what to do with the data once the period has passed.
- If you are not sure of the security measures in place or whether you need to implement ones.

- If you suspect or there has been a data breach. The school is under a legal obligation to report data breaches to the ICO immediately. Do not delay in reporting. Failing to do so can have significant consequences and penalties.
- If you are not clear about any of the school's privacy notices.
- If you are not sure about any confidentiality or disclosure obligations.
- If you are unclear about the school's retention schedule.
- If you are not sure about the rights of a data subject. A data subject is the living identifiable person whose data we hold.
- If a new system is implemented or activity takes place which requires an assessment of the data protection implications (data protection impact assessment), such as when a new contractor is appointed to deal with IT services.

Action plan

Procedures and practice

The following practices will be applied within the school:

- Policies and procedures will be reviewed and updated to ensure GDPR compliance.
- Compliance steps taken will be documented and retained.
- Staff will receive appropriate training on their obligations under the GDPR.
- All personal data will be fairly obtained in accordance with the privacy notices and lawfully processed.
- The amount of data held by the school will be reduced to a minimum.
- Data held by the school will be routinely assessed to consider whether it still needs to be kept or not and complies with the school's retention schedule. Documents that no longer need to be kept must be confidentially destroyed.
- Personal data held by the school will be securely stored and sent by secure means.
- Every effort will be made to ensure that the data held is accurate, up-to-date and that inaccuracies are corrected without unnecessary delay.
- Data breaches will be reported to the DPO immediately as will any queries or concerns regarding GDPR compliance.

Auditing

The school must be aware of *all* the personal data it holds, be it electronic or paper. Therefore:

- A register will be kept by the school DPO, detailing the types of personal data held, where and by whom. The register will be added to as and when new data is generated. This register will be checked by all team leaders each year to allow team members/colleagues to revise the list of types of data that they hold and manage.

- The length of time that individual documents need to be kept will be assessed using the IRMS Schools Toolkit <http://irms.org.uk/page/SchoolsToolkit>
- Audits will take place in line with the timetable for information security management. The audit will be completed by the DPO.

Risk assessment

The school/DPO will regularly carry out a risk assessment to establish what security measures are already in place and whether or not they are the most appropriate and cost effective available. The school's DPO is also the information risk officer, and s/he is responsible for the completion of the risk assessment.

The ICO provides guidance on Data Protection Impact Assessments at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments>.

Monitoring and reviewing

The policy will be monitored and evaluated regularly taking into account any incidents which occur, technological developments which might need a change in the policy or changes in legislation.

Reviewing

The policy will be discussed and reviewed annually as part of the governors' rolling programme of reviews.

This privacy notice advises parents, carers and guardians of the school's data protection responsibilities on the collection and processing of pupil's personal information.

You are being provided with this notice because you can exercise your child's data protection rights on their behalf. Current guidelines state that when your child is older (usually when they reach the age of 13) they may be considered mature enough to exercise their own data protection rights.

This notice provides details about:

- The personal information we collect on pupils.
- How we collect that personal information.
- What we do with the personal information.
- Your rights in relation to any personal information held and processed by the school.

We have appointed **Kate Hartill, Acting Headteacher** as the person with responsibility for ensuring that pupils' personal information is held and processed in the correct way. She can be contacted at admin@reay.lambeth.sch.uk Questions about this policy, or requests for further information, should be directed to her.

What is personal information and what does processing mean?

Personal information is any information that relates to your child that can be used directly or indirectly to identify your child.

This includes information such as their name, date of birth and address as well as information relating to their exam results, medical details and behaviour records. This may also include sensitive personal information such as their religion or ethnic group, photos and video recordings.

Personal information and processing are defined as follows:

- Personal data means any information relating to an identified or identifiable natural person (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 (GDPR article 4).
- Special categories of personal data means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric/genetic data (GDPR article 9).
- Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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 (GDPR article 4).

Data protection principles

We process personal data about pupils in accordance with the following data protection principles:

- We process personal data lawfully, fairly and in a transparent way.
- We collect personal data only for specified, explicit and legitimate purposes.
- We process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- We keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- We keep personal data in a form which permits identification from personal data for no longer than is necessary for the purpose of the processing or, if for longer periods, for such reasons as permitted by the GDPR.
- We adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

In our privacy notices, we tell individuals the reasons for processing their personal data, how we use such data and the legal basis for processing. We will not process personal data of individuals for reasons other than the stated purpose or purposes.

Where we process special categories of personal data or criminal records data to perform obligations, this is done in accordance with a policy, or for legal reasons. We will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Our legal basis (grounds) for using pupils' personal data

There are several reasons why we hold, process and share pupils' personal data. Under data protection laws, the lawful reasons for processing personal data include:

- Consent.
- For the performance of a contract.
- To comply with a legal obligation.
- To protect the vital interests of the pupil or another person.
- For a task carried out in the public interest.
- For a legitimate interest of the school or one of the organisations it shares data with (eg legal adviser) except where those rights are overridden by the interests or fundamental rights and freedoms of the data subject which require protection, particularly in the case of a child.

Sometimes the handling of pupils' personal data falls within several of the above lawful grounds.

Consent

We may ask for your consent to use your child's information in certain ways. If we ask for your consent to use your child's personal data, you can take back this consent at any time. Any use of your child's information before you withdraw your consent remains valid. For example, we **current use consent for the use of photographs for the school website, twitter, etc.,**

Performance of a contract

On some occasions, the school will process pupils' personal data for the performance of a contract.

Legal obligation

This is where we need to use pupils' personal data to comply with a legal obligation.

Statutory reporting requirements to the Department for Education (DfE) are included within this section. As is disclosing information to third parties such as the courts or the police where we are legally obliged to do so.

Extract from the Data Protection Toolkit regarding safeguarding at www.gov.uk/government/publications/data-protection-toolkit-for-schools.

'GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need.

The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent (DPA, Part 2,18; Schedule 8,4).

When designated safeguarding leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file.

All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place.'

Vital interests

This legal basis can be used where, for example, we need to disclose information about pupils to prevent them or someone else from being seriously harmed or killed. An example can include providing information to a medical professional about a pupil in circumstances where they are unable to provide the information themselves or you are unable to. It may cover an emergency situation.

Public interest

We consider that we are acting in the public interest when providing education.

Specifically, we have a public interest in:

- Providing an education.
- Fulfilling our safeguarding obligations and investigating complaints that may be directly connected with you or may require access to your personal data when investigating complaints by others.
- Promoting the interests of the school.
- Managing the school efficiently.

Legitimate interests

We have many legitimate interests for which we hold, retain, process and share pupils' personal data. This ground is therefore used for a large number of reasons. The GDPR states that the exception to using this ground is where it is detrimental to a pupil's rights.

Why do we collect and process pupils' personal data?

We use pupils' personal data to:

- Support pupil learning.
- Monitor and report on pupil progress.
- Provide appropriate pastoral care.
- Assess the quality of our services.
- Comply with the law regarding data sharing.

How do we obtain personal data?

We obtain personal data in a variety of ways. Some of the information comes from the admissions forms and acceptance forms which you supply to us. This can contain information about you as well as your child and the same principles contained in this notice apply regarding your personal data. We also receive information about pupils from other schools and agencies, such as healthcare professionals. Data is also obtained from your child, their teachers and other pupils.

With whom do we share pupils' personal data?

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 DfE on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

Pupils' data, where it is reasonable to do so, may also be shared with other professionals contracted by the school such as legal and professional advisers or insurers. In addition, a data security contract with a third-party IT services provider or as part of cloud-based storage may also process your personal data for the purpose of securely holding and protecting your data.

The National Pupil Database (NPD)

The NPD is owned and managed by the DfE. It 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 DfE. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities (LAs) 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 www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

Third parties

The DfE 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 DfE has robust processes in place to ensure the confidentiality of our data is maintained. There are stringent controls in place regarding access to and use of the data. Decisions on whether the 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 the requested data.
- 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.

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

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

Pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil information to our LA and/or provider of youth support services, because 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 such as:

- Youth support.
- Careers advice.
- Post-16 education and training providers.

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

Further examples of why we collect, hold and share pupils' personal data

Here are some further examples of why we collect, hold and share pupils' personal data. If you would like more information about any of these, please contact the school.

- We may need to share information about your child's health and wellbeing with those who have responsibility for pupil welfare.
- We need to tell all appropriate members of staff if your child has specific medical needs.
- We need to tell all appropriate members of staff if your child might need extra help with some tasks.
- We may need to provide information containing your child's personal data to other schools and colleges. We may need to pass on information which they need to look after your child. For example, how well your child has behaved at other schools and their test results.

- We may need to share data with external examination boards.
- Where we have the right to do so, we may share your child's academic and behaviour records with you or their guardian.
- We will only share your child's information with other people and organisations when we have a legitimate reason to do so.
- We are required to share information about our pupils with our LA and the DfE under the Education (Information About Individual Pupils) (England) Regulations 2013.
- Sometimes we need to share information with the police or our legal advisers to help with an inquiry. For example, safeguarding issues or injuries.
- We might need to share pupils' information with consultants, experts and other advisers who assist us in the running of the school, if this is relevant to their work.
- On occasions external consultants/contractors may have temporary access to personal data held by the school. For example, IT consultants might be granted temporary access to pupils' personal data in order to fulfil their contract(s). Access will only be granted to consultants who have demonstrated compliance with the school's data protection standards.
- The school uses various IT systems. This may include using cloud-based storage systems to hold pupil data. Before use, the school ensures that adequate security measures are in place.
- We may need to share some information with our insurance provider to ensure we maintain cover or to process any claims.
- We may need information about any court proceedings or judgements concerning your child. This is so that we can safeguard your child's welfare and the welfare of other pupils at the school.
- We may monitor your child's use of the school's email, internet and other electronic devices provided by the school eg iPads. We monitor in order to ensure appropriate use of these technologies and to confirm your child is not putting themselves at risk of harm.
- We have CCTV in operation to make sure the school sites are safe. CCTV is not used in private areas such as changing rooms.
- We may use photographs or videos of your child on our website, social media sites, newsletters and publications as part of our advertising of the school.
- We publish our exam results and other news on the website. We also send articles, photographs and videos to local and national news outlets to celebrate the school's successes.
- Sometimes we use photographs and videos to support curriculum activities, for example, to provide feedback on a presentation your child has given.

Automated decision-making and profiling

We do not make automatic decisions or undertake automated decisions regarding individuals to evaluate certain information about an individual (profiling)

Special categories of personal data

We must also comply with an additional condition where we process special categories of personal data. These special categories include: personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic information, biometric information, health information, and information about sex life or orientation.

Some of the reasons we process such data on pupils include:

- Legal claims. The processing is necessary for the establishment, exercise or defence of legal claims. This allows us to share information with our legal advisers and insurers.
- Medical purposes. This includes medical treatment and the management of healthcare service.
- For compiling census data as required by law.

How do we protect pupils' personal data?

We take the security of pupils' personal data very seriously. We have internal policies and controls in place to try to ensure that data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where we engage third parties to process personal data on our behalf, they do so based on written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data. For example, we ensure the school uses encrypted devices, uses passwords, virus protection and has appropriate firewalls.

Sending information to other countries

With cloud-based storage and some other services sometimes being supplied outside the UK, personal data can be sent to other jurisdictions.

Our servers and storage systems **are** based in the EU or the European Economic Area (EEA) and we have ensured that appropriate safeguards are in place to protect your pupils' personal data.

How long do we keep pupils' personal data?

We keep pupils' personal data for the time they are at our school. We will also keep certain information after pupils have left the school. A copy of our Retention Schedule is available from the school website.

What rights do you have in relation to your child's information?

You will have the following rights in relation to your child's personal data. Some of these rights are new since 25 May 2018.

- The right of access to the personal data and supplementary information. This right is to enable you to be aware of and verify the lawfulness of the personal data we are processing.
- The right to rectification. This right allows you to have personal data rectified if it is inaccurate or incomplete.

- The right to erasure. This is also known as the ‘right to be forgotten’. This is not an absolute right and applies in specific circumstances.
- The right to restrict processing. This right applies in circumstances where, for example, the data subject contests the accuracy of the data or challenges the public interest or legitimate interest basis. Further guidance can be obtained from the ICO’s website.
- The right to data portability. This allows individuals to obtain and reuse their personal data for their own purposes.
- The right to object. Individuals have the right to object to:
 - Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority.
 - Direct marketing.
 - Processing for scientific/historical research and statistics.
- Rights in relation to automated decision making and profiling.

There are specific rights in relation to a child’s personal data. Further guidance and advice on the above rights can be obtained from the ICO’s website <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>.

If you have a concern about the way we are collecting or using your child’s personal data, we ask that you raise your concern with us in the first instance by contacting **Kate Hartill, Acting Headteacher or the Data Protection Officer** at dpo@ascentassets.com If you would like to exercise any of the above rights please download the data subject’s rights application form on the website.

Alternatively, you can contact the Information Commissioner’s Office at <https://ico.org.uk/concerns> to raise any issues you have.

Reviewing

Date agreed by governing board on	Signature of Chair or Vice Chair
Date agreed for review:	Frequency of Review Annually
Review Responsibility Full Governing Board	

