Data Protection Policy

Prepared using:

- 2015 DfE publication - Information sharing advice for safeguarding practitioners;
- Subject access code of practice version 1.2;
- Education Act 1996. The EU general data protection regulation 2016/679;
- Section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments;
- Data Protection Act 2018;
- GDPR - Articles 6 and 9;
- https://www.gov.uk/education/data-collection-and-censuses-for-schools
- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- DFE Information sharing in schools and colleges, July 2018
- DFE Working together to safeguard children, July 2018
- Keeping Children Safe in Education, September 2018

The Data Protection Act 2018 controls how personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

General Statement

The Iona School collects and uses personal information (referred to in the Data Protection Act as personal data) about staff, pupils, parents and other individuals who come into contact with them. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

The school is registered as a Data Controller, with the Information Commissioner's Office (ICO). Details are available on the ICO website.

Purpose

This policy sets out how the school deals with personal information correctly and securely and in accordance with the Data Protection Act 2018, and other related legislation, including GDPR.

This policy applies to all personal information however it is collected, used, recorded and stored and whether it is held on paper or electronically.

All school staff and governors involved with the collection, use, processing or disclosure of personal data will be aware of their duties and responsibilities and will adhere to this policy.

What is GDPR?

The GDPR is a new data and privacy security legislation which was developed by the European Parliament and Council for the protection of data rights of the EU citizens. Companies (including websites, mobile, and desktop apps etc.) that do business transactions with EU citizens are affected by this regulation.

On 25th May 2018, the GDPR replaced the existing data protection law i.e. the Data Protection Directive that has been in effect since 1998. If your company collects or processes the data of EU citizens, you are required to comply with this regulation.

One of the key aims and requirements of the GDPR is to keep EU citizens informed of how businesses collect, use, share, secure and process their personal data.

Under the GDPR, you are required to inform your customers about why you are processing their data and for how long will you store it. You must tell them in plain and clear words how you use their data.

What is Personal Information / Data?
Personal information or data is information which relates to a living individual who can be identified from that data, or from that data in addition to other information available to them. Personal data includes (but is not limited to) an individual's name, address, date of birth, photograph, bank details and other information that identifies them.

What is Sensitive Personal Data?
Sensitive personal data includes information as to an individual's racial or ethnic origin, their political opinions, religious beliefs or beliefs of a similar nature, whether they are a member of a trade union, their physical or mental health or condition, sexual life, the commission or alleged commission of an offence and any proceedings for an offence committed or alleged to have been committed by them, the disposal of those proceedings or the sentence of any court in such proceedings.

Data Protection Principles
The Data Protection Act 2018 establishes eight principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purpose;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data, subject under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the EEA, unless that country or territory ensures an adequate level of data protection.

Commitment
The school is committed to maintaining the above principles at all times. Therefore, the school will:

- Inform individuals why personal information is being collected;
- Inform individuals when their information is shared, and why and with whom unless the Data Protection Act provides a reason not to do this;
- Obtain consent before processing Sensitive Personal Data, even if consent is implied within a relevant privacy notice, unless one of the other conditions for processing in the Data Protection Act applies;
- Check the accuracy of the information it holds and review it at regular intervals;
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in;

- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
- Ensure that personal information is not retained longer than it is needed;
- Ensure that when information is destroyed that it is done so appropriately and securely;
- Share personal information with others only when it is legally appropriate to do so;
- Comply with the duty to respond to requests for access to personal information, known as Subject Access Requests;
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards;
- Ensure all staff and Trustees are aware of and understand these policies and procedures.

Sharing information regarding safeguarding must be read in conjunction with the Safeguarding Policy.

1. Remember that the Data Protection Act 1998 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.

2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice from other practitioners if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible. The Designated Safeguarding Lead must always be consulted on sharing children's information.

4. Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is good reason to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared.

5. Consider safety and well-being. Base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.

6. Necessary, proportionate, relevant, adequate, accurate, timely and secure. Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

When and How to Share Information

When asked to share information, you should consider the following questions to help you decide if and when to share. If the decision is taken to share, you should consider how best to effectively share the information.

When
Is there a clear and legitimate purpose for sharing information?
- Yes – see next question
- No – do not share

Does the information enable an individual to be identified?
- Yes – see next question
- No – you can share but should consider how is the information confidential?

Do you have consent?
- Yes – you can share but should consider how is the information confidential?
- No – see next question

Is there another reason to share information such as to fulfil a public function or to protect the vital interests of the information subject?
- Yes – you can share but should consider how is the information confidential?
- No – do not share

How
- Identify how much information to share;
- Distinguish fact from opinion;
- Ensure that you are giving the right information to the right individual;
- Ensure where possible that you are sharing the information securely;
- Inform the individual that the information has been shared if they were not aware of this, as long as this would not create or increase risk of harm.

All information sharing decisions and reasons must be recorded. If at any stage you are unsure about how or when to share information, you should seek advice and ensure that the outcome of the discussion is recorded. If there are concerns that a child is suffering or likely to suffer harm, then follow the relevant procedures in the Safeguarding Policy without delay.

For requests for information from parents that may cause harm to either children or staff, this should not be disclosed.

The Data Protection Act's subject access code of practice (v 1.2) states that in deciding what information to supply to a Subject Access Request (SAR) you need to have regard to the general principles about exemptions. It is a matter for you to decide whether or not to use an exemption.

Data Breach

What is a personal data security breach?
A personal data security breach is any event that has the potential to affect the confidentiality, integrity or availability of personal data held by the school in any format. Personal data security breaches can happen for a number of reasons, including:

- The disclosure of confidential data to unauthorised individuals;
- Loss or theft of portable devices or equipment containing identifiable personal, confidential or sensitive data e.g. PCs, USB, mobile phones; Laptops, disks etc.;

- Loss or theft of paper records;
- Attempts to gain unauthorised access to computer systems, e.g. hacking;
- Records altered or deleted without authorisation from the data "owner";
- Viruses or other security attacks on IT equipment systems or networks;
- Breaches of physical security e.g. forcing of doors on filing cabinet containing confidential information;
- Confidential information left unlocked in accessible areas;
- Insecure disposal of confidential paper waste;
- Leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information;
- Publication of confidential data on the internet in error and accidental disclosure of passwords;
- Misdirected emails or faxes containing identifiable personal, confidential

What to do in the case of a data breach

If there is a data breach in any way, this must be recorded on an all incident report form, then given to the Data Officer (School Business Manager) within 24 hours. The form must contain the following:

- If a personal data security breach has taken place; if so:
- What personal data is involved in the breach;
- The cause of the breach;
- The extent of the breach (how many individuals are affected);
- The harms to affected individuals that could potentially be caused by the breach; and
- How the breach can be contained.

They will ascertain the risk of the breach using the following scale:

Rating	**0**	**1**	**2**	**3**	**4**	**5**	**6**
Reputation	No significant reflection on any individual or body Media interest very unlikely	Damage to an individual's reputation. Possible media interest (eg prominent member of the College /trustee involved)	Damage to class/office/kg reputation. Some local or subject specific school media interest that may not go public	Damage to school reputation / Low key local media coverage	Damage to school reputation local media coverage	Damage to school reputation/ national media coverage	Monetary Penalty Imposed by ICO
Individuals potentially affected	Minor breach of confidentiality. Only a single individual affected	Potentially serious breach. Less than 5 people affected or risk assessed as low (eg files were encrypted)	Serious potential breach & risk assessed high (eg unencrypted sensitive/health records lost) Up to 20 people affected	Serious breach of confidentiality eg up to 100 people affected and/or identifiable or particularly sensitive ie redundancies, restructuring	Serious breach with either particular sensitivity (eg sexual or mental health details, identifying information of vulnerable people), or up to 1000 people affected	Serious breach with potential for ID theft or over 1000 people affected	Restitution to injured parties Other Liabilities Additional Security Legal Costs

We only have to notify the ICO of a breach if it could result in a risk to the rights and freedoms of individuals. For example if it could result in discrimination, damage to reputation, financial loss or any other significant economic or social disadvantage.

It is compulsory that all data breaches which are likely to have a detrimental effect on the data subject are reported to the ICO within 72 hours.

We will consider the potential adverse consequences for individuals, i.e. how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be. The information provided at Stage 1 on the all incident report form will assist with this stage.

- Assess the risks and consequences of the breach:
    - Risks for individuals:
        - What are the potential adverse consequences for individuals?
        - How serious or substantial are these consequences?
        - How likely are they to happen?

    - Risks for the School
        - Strategic & Operational
        - Compliance/Legal
        - Financial
        - Reputational Continuity of Service Levels

- Consider what type of data is involved, how sensitive is it? Were there any protections such as encryption? What has happened to the data? If data has been stolen it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged this poses a different type and level of risk;
- Consider how many individuals' personal data are affected by the breach. It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment;
- Consider the individuals whose data has been breached. Whether they are staff, students, or suppliers will to some extent determine the level of risk posed by the breach and therefore, the actions in attempting to mitigate those risks;
- Consider what harm can come to the affected individuals. Are there risks of physical safety or reputation, of financial loss or a combination?
- Consider if there are wider consequences to consider such as a loss of public confidence in an important service the school provides; and
- Determine, where appropriate, what further remedial action should be taken on the basis of the incident report to mitigate the impact of the breach and prevent repetition.

The investigators will prepare an **incident report** setting out (where applicable):

- a summary of the security breach;
- the people involved in the security breach (such as staff members, students, contractors, external clients);
- details of the information, IT systems, equipment or devices involved in the security breach and any information lost or compromised as a result of the incident;
- how the breach occurred;
- actions taken to resolve the breach;
- impact of the security breach;

- unrealised, potential consequences of the security breach;
- possible courses of action to prevent a repetition of the security breach;
- side effects, if any, of those courses of action; and
- recommendations for future actions and improvements in data protection as relevant to the incident.

Notification

On the basis of the evaluation of risks and consequences, the Lead Investigator in consultation with the college and trustees and others involved in the incident as appropriate, will determine whether it is necessary to notify the breach to others outside the school or nursery. For example:

- the Police
- individuals (data subjects) affected by the breach
- the Information Commissioner's Office
- other bodies such as Department for Employment and Learning
- Our PR company
- the College's insurers
- bank or credit card companies
- trade unions
- external legal advisers

As well as deciding **who** to notify, the Lead Investigator must consider:

- **What** is the message that needs to be put across?

In each case, the notification should include as a minimum:

- a description of how and when the breach occurred;
- what data was involved; and
- what action has been taken to respond to the risks posed by the breach.

When notifying individuals, the Lead Investigator should give specific and clear advice on what steps they can take to protect themselves, what the school is willing to do to assist them and should provide details of how they can contact the school for further information (e.g. helpline, website).

Use of Portable Devices

The school recognises that personal data may be accessed by users out of school, however, we fully prohibit the use of **memory sticks.**

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage;
- Users must take particular care that laptops which contain personal data must not be accessed by other users (e.g. family members) when out of school;
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;

- if secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of Data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

- The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Burning or shredding is a good way!
- Electronic files must be securely overwritten, in accordance with government guidance and other media such as CD/DVD/Memory sticks must be incinerated or otherwise disintegrated for data, with any references to that deleted off the system. Remember to empty your recycle bin!

A Destruction Log is kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Privacy Notice - Parents, Pupils and Visitors

Why do we Collect, Share and Hold Pupil Information
Why do we collect and use pupil information? We collect and use pupil information under the Education Act 1996. The EU General Data Protection Regulation 2016/679 (GDPR) took effect from May 2018. Note in particular Article 6 and 9 of the GDPR.

Article 6
Processing is necessary for compliance with a legal duty to which the controller is subjected.

Article 9
For substantial public interest on a legal basis.

https://www.gov.uk/education/data-collection-and-censuses-for-schools

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

The categories of pupil information that we collect, hold and share include:
- Personal information (such as name and address);
- Any relevant medical information;

- Special educational needs;
- Exclusions and behavioural information;
- Assessment information;
- Characteristics (such as ethnicity, language, nationality, country of birth);
- Attendance information (such as sessions attended, number of absences and absence reasons).

Collecting Pupil Information
Whilst the majority of pupil information provide by parents is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the GDPR, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing Pupil Data
We hold pupil data until they reach 25 years of age.

Who Do We Share Pupil Information With?
We routinely share pupil information with:

- schools that pupils attend after leaving the school;
- our local authority;
- the Department for Education (DfE).

Why We Share Pupil Information
We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so. We are required to share safeguarding information with the LA and any school the child moves on to.

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

The school must also comply with an additional condition where it processes special categories of personal information. These special categories include personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic information, biometric information, health information, and information about sexual life or orientation.

Substantial Public Interest
The processing is necessary for reasons of substantial public interest.

Vital Interests
To protect the vital interests of any person where that person cannot give consent, for example, if they are seriously hurt and are unconscious.

Legal Claims
The processing is necessary for the establishment, exercise or defence of legal claims. This allows us to share information with our legal advisors and insurers.

Medical Purposes
This includes medical treatment and the management of healthcare services.

We may ask for your consent to use your information in certain ways. If we ask for your consent to use your personal information you can take back this consent at any time. Any use of your information before you withdraw your consent remains valid.

Requesting Access to your Personal Data
Under data protection legislation, parents have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the School Business Manager.

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

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with the School Business Manager in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/.

Our Legal Grounds for Using your Information
This section contains information about the legal basis that we are relying on when handling your information.

Legitimate interests
This means that the processing is necessary for legitimate interests except where the processing is unfair to you. The school relies on legitimate interests for most of the ways in which it uses your information.

Specifically, the school has a legitimate interest in:
- Providing educational services to your child;
- Safeguarding and promoting the welfare of your child (and other children);
- Promoting the objects and interests of the school. This includes fundraising. It also includes making sure that we are able to enforce our rights against you, for example, so that we can contact you if unpaid school fees are due;
- Facilitating the efficient operation of the school; and
- Ensuring that all relevant legal obligations of the school are complied with.

In addition, your personal information may be processed for the legitimate interests of others, e.g. another school will have a legitimate interest in knowing if you have not paid sSchool fees that are due to us.

If you object to us using your information where we are relying on our legitimate interests as explained above please speak to the School Business Manager.

Necessary for a Contract
We will need to use your information in order to perform our obligations under our contract with you. For example, we need your name and contact details so that we can update you on your child's progress and so that we can contact you if there is a concern.

Legal Obligation
Where the school needs to use your information in order to comply with a legal obligation, for example to report a concern to Children's Services. We may also have to disclose your information to third parties such as the courts, the local authority or the police where legally obliged to do so.

Vital Interests
For example, to prevent someone from being seriously harmed or killed.

Public Interest
The school considers that it is acting in the public interest when providing education.

Staff

This policy is compulsory for all school employees and contract staff.

The Iona School is committed to being a responsible user of personal data and compliance with this procedure and other relevant procedures related to an employee's role will ensure that both employer and employee meet obligations under the Act. If employees are unsure as to the application of this procedure to the information held as part of their role, they should contact the School Business Manager for further guidance.

This procedure does not form part of a contract of employment and does not give rise to any contractual rights to employees. The Iona School may issue further guidance or make amendments to this procedure from time to time.

The aim of this procedure is to assist the school to meet its obligations under the data protection requirements and to regulate its use of information relating to employees and others who work for it. For ease of reference, the procedure refers to 'employees' but it applies equally to others working for The Iona School.

The Iona School's Obligations
The school will ask each employee to consent to our processing of information relating to them in line with the provisions set out in this procedure. 'Processing' is the term used in the Data Protection Act to refer to the collection, use, disclosure, holding and erasure of information. It is therefore important for employees to read the rest of this procedure to ensure that they are aware of the nature of the information that the school holds about employees and the reasons for needing to process this information.

Employee Personal Information
Personal information is held on personal paper files and electronic databases, which are kept securely within the school. The categories of information held on personal files may include, amongst other items, home address, contact telephone numbers, emergency contact details, marital status, details of salary and benefits and bank details.

It is not possible to list every type of information which may be held by the school about every employee and so these are only examples of the usual type of information and do not constitute an exhaustive list. This sort of information is known as 'personal data' under the Data Protection Act (DPA).

The DPA also recognises a category of information known as sensitive personal data. Sensitive personal data is information which relates to racial or ethnic origin, political opinions, religious beliefs, trade union memberships, physical or mental condition, sexual life or orientation, any criminal offence or related proceedings. The most likely information which the school collects and processes on an employee's behalf, which falls into this category, is information relating to health. The purpose of keeping this information is to administer Statutory Sick Pay, monitor and manage sickness absence and to comply with health and safety obligations and the Equality Act 2010.

Retaining Employee Information
Access to personal files is limited to the school leaders and, in some circumstances, Trustees. The school will take steps to ensure that the information it holds on employees is accurate and up-to-date. The school will also take steps to ensure that it does not keep any information about employees for longer than is necessary. It may, for example, keep details of employees for a reasonable time after they have left the school in order to ensure that benefits have been properly administered, to give references if requested to do so, to ensure that school's tax obligations have been satisfied and to deal with any tribunal or other court proceedings.

Transfer of Employee Information
The school may make some information about employees available to legal and regulatory authorities (such as the Inland Revenue), accountants, auditors, lawyers and other outside professional advisers and product service providers. In this case the school will ensure that the recipients of the information comply with the contents of this procedure.

Employee Rights under the Data Protection Rules
The Data Protection Act gives employees (and anyone else about whom personal data is held) specific rights in relation to the information that is held about them. Some of these rights are summarised below, but if an employee would like any further information, please contact the School Business Manager.

Under the Data Protection Act employees are able to:

- Obtain confirmation that the school holds personal information about them, as well as a written description of the information, the purposes for which it is being used, the sources of the information and the details of any recipients.
- Access the personal information which is held about them. It is important to note that this is not an absolute right to review all the information that is held, as there are various exceptions to this right contained in the Data Protection Act. One of the most important exceptions is that employees may not be able to access the information if it reveals personal information about someone else.
- In certain circumstances employees can ask for the deletion or rectification of information which the school holds about them which is not accurate.

If employees wish to see their personal data, please contact the School Business Manager.

Employee Responsibilities under the Data Protection Rules
As well as having rights under the Data Protection Act, employees should comply with the data protection rules set out in this policy.

Other People's Personal Information
If, as a part of an employee's role, they hold any personal information about a colleague or anyone else, then they need to take steps to ensure that they are following guidelines set out below. Please note the following guidelines which apply equally to documents containing personal information, which are kept in files, as well as information which is kept on an electronic database.

- All personal information must be kept securely and remain confidential;
- You should not keep personal information about people which you no longer need or which is out of date or inaccurate. You should therefore review any personal information that you hold from time to time, bearing these principles in mind.

Staff Privacy Notice

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

- Personal information such as name, address, teacher number, national insurance number;
- Special categories of data including characteristics information such as gender, age, ethnic group;
- Contract information such as start dates, hours worked, post, roles and salary;
- Work absence information such as number of absences and reasons;
- Qualifications and, where relevant, subjects taught;
- Medical information;
- Addresses;
- Payroll information;
- Criminal activities (staff discrimination disclosure);
- Overseas checks;
- DBS certificate number

Why we Collect and Use this Information

We use employee data to:

- enable the development of a comprehensive picture of the staff and how they are deployed;
- inform the development of recruitment and retention policies;
- enable individuals to be paid;
- ensure that DfE and Ofsted regulations are met.

Collecting this Information

Whilst the majority of information employees provide to school is mandatory, some is provided on a voluntary basis. In order to comply with data protection legislation, the school will inform employees whether they are required to provide certain information or if they have a choice in this.

Storing this Information

The school holds employee records for at least 6 years after the employee leaves the school.

Who we Share this Information with

The school does not share information about employees with anyone without consent unless the law and our policies allow the school to do so.

We routinely share this information with:

Our Local Authority

The school is required to share information about our employees with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

The Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins employee policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

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

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

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

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

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

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

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

Requesting Access to your Personal Data
Under data protection legislation, employees have the right to request access to information about themselves that the school holds. To make a request for your personal information, contact the School Business Manager**.**

Employees also have the right to:

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

If employees have a concern about the way the school is collecting or using their personal data, please speak with the School Business Manager. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/.

Further Information
If you would like to discuss anything in this privacy notice, please contact the School Business Manager.

Issue Date
This policy takes effect from February 2013. This policy was reviewed in June 2020.

Review Date
This policy will be reviewed and revised by the School Business Manager on a three yearly basis.

Endorsement
Full endorsement to this policy is given by:

Name:	Mr Martin Taylor
Position:	Trustee
Signed:	
Date:	

Related Policies
- DBS Policy
- Safeguarding Policy