

Data protection policy 2022

Marish Academy Trust



Approved by: Strategic Board

Date: 17/04/2022

Last reviewed on: April 2022

Next review due by: April 2024

Contents

1. Aims	2
2. Legislation and guidance	2
3. Definitions	3
4. The data controller	4
5. Roles and responsibilities	4
6. Data protection principles	5
7. Collecting personal data	5
8. Sharing personal data	5
9. Subject access requests and other rights of individuals	6
10. Parental requests to see the educational record	8
11. Biometric recognition systems	8
12. CCTV	8
13. Photographs and videos	8
14. Data protection by design and default	8
15. Data security and storage of records	9
16. Disposal of records	9
17. Personal data breaches	9
18. Training	Error! Bookmark not defined.
19. Monitoring arrangements	10
20. Links with other policies	Error! Bookmark not defined.
Appendix 1: Personal data breach procedure	11
Appendix 2: Marish Academy Trust privacy notice	14
Appendix 3: MAT HR Privacy Notice	10

1. Aims

Marish Academy Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [Data Protection Act 2018 \(DPA 2018\)](#)

It is based on guidance published by the Information Commissioner's Office (ICO) on the [UK GDPR](#).

It also reflects the ICO's [guidance](#) for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
<p>Personal data</p>	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"> ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
<p>Special categories of personal data</p>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes ● Health – physical or mental ● Sex life or sexual orientation
<p>Processing</p>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
<p>Data subject</p>	<p>The identified or identifiable individual whose personal data is held or processed.</p>
<p>Data controller</p>	<p>A person or organisation that determines the purposes and the means of processing of personal data.</p>

Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Marish Academy Trust which consists of Marish Primary School and Willow Primary School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

Marish Academy Trust is registered as a data controller with the ICO and pays its annual data protection fee to the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Mrs Nicola Cook and she is contactable via nicola@schoolsdp.com

5.3 Executive Headteacher

The Executive headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not, they have a lawful basis to use personal data in a particular way

- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our schools must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how Marish Academy Trust aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's record retention schedule which is based upon the

[Information and Records Management Society's toolkit for schools](#) .

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
 - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
 - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
 - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO

- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

As an Academy there is no automatic parental right of access to the educational record. However, the Trust will consider any Subject Access Requests.

11. Biometric recognition systems

Marish Academy Trust does not have Biometric recognition systems in place.

12. CCTV

We use CCTV in various locations around the academy sites to ensure it remains safe. We will adhere to the ICO's [code of practice](#) for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Trust Data Network Manager by email Brendan.Rossiter@marishandwillow.co.uk or call 01753819900.

13. Photographs and videos

As part of our everyday activities, we may take photographs and record images of individuals within our academy schools.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within the Trust on notice boards and in school brochures, newsletters, leaflets etc.
- Outside of an academy by external agencies such as the school photographer, newspapers, campaigns
- Online on our schools websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our safeguarding policy and home school agreement for more information on our use of photographs and videos.

14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)

- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment, (see acceptable use of the internet agreement)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of an Academy laptop containing non-encrypted personal data about pupils

18. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy in liaison with the Academy Leadership Team. It will be reviewed annually but only ratified by the strategic board of the governing body every 2 years unless there are major changes to be incorporated.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Child Protection & Safeguarding Policy
- E Safety Policy & ICT Acceptable Use Agreement
- Home School Agreement
- Staff Handbook & Code of Conduct
- Safer Recruitment Policy

Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust's secured computer system.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the Trust's secured computer system

The DPO, and Executive headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Below is a list that is not intended to be exhaustive but lists actions we will take for different types of sensitive personal data processed by an academy. For example:

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other risks of potential data security breaches we have already minimized are shown below:

- Details of pupil premium interventions for named children being published on the school website-; (No pupil level data is ever uploaded to the website.)
- Non-anonymised pupil exam results or staff pay information being shared with governors- (This cannot happen as only anonymized results/finance documents shown or discussed with Governors.)
- An academy laptop containing non-encrypted sensitive personal data being stolen or hacked- (Sensitive data is not stored on laptops.)
- The school's cashless payment provider being hacked and parents' financial details stolen- (External risk which the system provider mitigates against by complying fully with GDPR and ICT security legislation.)

- The school's payroll provider being hacked and staffs' financial details stolen- (External risk which the system provider mitigates against by complying fully with GDPR and ICT security legislation.)



Data Protection Act 1998: How we use pupil information

This privacy notice explains how we collect, store and use personal data about pupils within our Trust. Marish Academy Trust, Swabey Road, Slough, SL3 8NZ is the data controller for the purpose of data protection law. Our data protection officer is Nicola Cook.

Personal data that we may collect, use, store and share (when appropriate) about your child includes, but is not restricted to:

- **Contact details, contact preferences, date of birth, identification documents**
- **Results of internal assessments and externally set tests**
- **Pupil and curricular records**
- **Exclusion information**
- **Attendance information**
- **Safeguarding information**
- **Details of any support received, including care packages, plans and support providers**

We may also collect, use, store and share (when appropriate) information about your child that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to, information about:

- **Any medical conditions we need to be aware of, including physical and mental health**
- **Photographs and CCTV images captured in school**
- **Characteristics, such as ethnic background or special educational needs**

We may also hold data about your child that we have received from other organisations, including other schools and social services. **We use the data listed to; support pupil learning, monitor and report on pupil progress, provide appropriate pastoral care, protect pupil welfare, assess the quality of our services, administer admissions waiting lists.**

Where you have given us consent to do so, we may send marketing information by email or text promoting school events, campaigns, charitable causes or services that may be of interest. You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by contacting us.

We keep personal information about your child while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary. Our retention schedule sets out how long we keep information about pupils. We have put in place appropriate security measures to prevent your child's personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We will dispose of your child's personal data securely when we no longer need it.

We do not share information about your child with any third party without consent unless the law and our policies allow us to do so.

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school and early years census. Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research. The information is securely collected from a range of sources including schools, local authorities and exam boards. The Department for Education may share information from the NPD with third parties, such as other organisations which promote children's education or wellbeing in England. These third parties must agree to strict terms and conditions about how they will use the data. For more information, see the Department's web page on how it collects and shares research data; www.gov.uk/data-protection-how-we-collect-and-share-research-data.

If you require a copy of the data we hold on you or your child please contact our data protection officer: Nicola Cook via the following email address: nicola@schoolsdpo.co.uk

Appendix 3: MAT HR Privacy Notice

MARISH ACADEMY TRUST



PRIVACY NOTICE FOR SCHOOL WORKFORCE

HOW MARISH ACADEMY TRUST USE SCHOOL WORKFORCE INFORMATION

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

- personal information (such as name, address, telephone numbers, email address, employee or teacher number, national insurance number, bank account number and emergency contact information)
- special categories of personal data including; characteristics information (such as gender, age, ethnic group and religious belief), any health conditions you have that we need to be aware of, sickness records, photographs and CCTV images captured in school, trade union membership.
- pre-employment and safeguarding checks (such as “Right to Work in the UK” information, DBS and Children’s Barred List outcome information, pre-placement medical questionnaire outcome information, employment references, overseas check outcome information, and Teacher Status Check outcome information)
- contract information (such as start dates, hours worked, post, roles, salary(payroll/pension) information, and continuous service dates)
- work absence information (such as number and type of absences and reasons)
- performance management, grievance, and conduct or disciplinary information [where applicable]
- settlement agreements, COT3 agreements, and claims to an Employment Tribunal or Employment Appeal Tribunal [where applicable]
- qualifications (and, where relevant, subjects taught).

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- manage recruitment processes and safer recruitment requirements
- enable individuals to be paid and receive pension at appropriate time
- manage work absence and other performance management and conduct or disciplinary related activities in accordance with the Marish Academy Trust’s policies and procedures

The lawful basis on which we process this information

We collect and use information under Article 6 and Article 9 of the GDPR, this enables the school to process information such as Departmental Censuses under the Education Act 1996 and other such data processes that relate education provision or payment of the individual. Further information is available at <https://www.gov.uk/education/data-collection-and-censuses-for-schools>

Collecting this information

While the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. To comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We keep personal information about you while you work at our school. We may also keep it beyond your employment at our school if this is necessary. We hold school workforce data in line with our Data Retention Guidelines, which are available upon request. We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

Who we share this information with

We routinely share this information with:

- our local authority
- the Department for Education (DfE)
- The Schools HR Co-operative
- Pupil Asset
- Medigold Health (Occupation Health Provider)
- Wellbeing Solutions Management (Counseling Service)
- Dataplan Education (Payroll Provider)

Why we share school workforce information

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

Local Authority

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

Department for Education (DfE)

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

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

The Schools HR Co-operative (“Schools HR”)

We share personal data, including special categories of personal data, with Schools HR for HR-related purposes, including:

- processing safer recruitment checks
- the administration of your employment contract (including calculation of continuous service dates for conditions of service and identifying long service award eligibility) enabling you to be paid, and for pension contributions to be made to a pension scheme [where applicable]
- enabling you to be paid, and for pension contributions to be made to a pension scheme [where applicable]
- supporting work absence policies and procedures (including sickness absences)

- managing your performance and conduct
- undertaking any grievance, disciplinary, or related investigations
- advising on, and responding to, employment-related matters (including settlement agreements, COT3 agreements, and claims in the Employment Tribunal and Employment Appeal Tribunal) [where applicable].

Pupil Asset

We share personal data, including special categories of personal data, with Pupil Asset database administration and technical support purposes, including:

- the administration of your workforce data
- ensuring you are paid the correct amount
- supporting the statutory return process (DfE censuses).

Medigold Health

We share personal data, including special categories of personal data, with Medigold Health for managing work absences and wellbeing support, including:

- assessing your fitness to work
- when required, referring you for an occupational health assessment or consultation
- supporting your attendance at work (including making any reasonable adjustments to support your return to work and/or ongoing attendance at work).

Wellbeing Solutions Management

We share personal data with Wellbeing Solutions to provide you with a confidential employee assistance programme (EAP), including:

- confirming your eligibility to access the EAP online portal and telephone helpline
- offering you confidential counseling and advice.

Please note: This service is confidential and Marish Academy Trust does not know which individual employees access this service and for what purpose or reason.

Data Plan Education

- enabling you to be paid, and for pension contributions to be made to a pension scheme [where applicable]
- supporting work absence policies and procedures (including sickness absences)

Data collection requirements

The Department for Education (DfE) collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the DfE, including the data that we share with them, visit <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 the DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

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

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

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>

To contact the DfE please visit:
<https://www.gov.uk/contact-dfe>

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information please contact our HR Team on hr@marishandwillow.co.uk

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
- claim compensation for damages caused by a breach of the Data Protection regulations.

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

Further information

If you would like to discuss anything in this privacy notice, please contact:
 Nicola Cook our Data Protection Officer via the following email address: nicola@schoolsdp0.com