



The Warriner Multi Academy Trust Data Protection policy

| | | |
|----------------------------|--------------|--|
| Approved by: | Trust Board | Date: 9 th December 2020 |
| Next review due by: | October 2021 | |

Contents

| | |
|--|----|
| 1. Aims..... | 2 |
| 2. Legislation and guidance | 2 |
| 3. Definitions | 2 |
| 4. The data controller | 3 |
| 5. Roles and responsibilities | 3 |
| 6. Data protection principles..... | 4 |
| 7. Collecting personal data..... | 4 |
| 8. Sharing personal data | 5 |
| 9. Subject access requests and other rights of individuals | 6 |
| 10. Biometric recognition systems..... | 7 |
| 11. CCTV | 8 |
| 12. Photographs and videos | 8 |
| 13. Data protection by design and default | 8 |
| 14. Data security and storage of records..... | 9 |
| 15. Disposal of records | 9 |
| 16. Personal data breaches | 9 |
| 17. Training..... | 10 |
| 18. Monitoring arrangements | 10 |
| 19. Links with other policies | 10 |
| Appendix 1: Personal data breach procedure | 11 |
| Appendix 2: Privacy notices | |

.....

1. Aims

The Warriner Multi 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 the [General Data Protection Regulation \(GDPR\)](#) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#).

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 GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#).

It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data.

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

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

3. Definitions

| Term | Definition |
|--|---|
| Personal data | Any information relating to an identified, or identifiable, individual. This may include the individual's: <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data• Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. |
| Special categories of personal data | Personal data which is more sensitive and so needs more protection, including information about an individual's: <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 |

| | |
|-----------------------------|---|
| Processing | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual. |
| Data subject | The identified or identifiable individual whose personal data is held or processed. |
| Data controller | A person or organisation that determines the purposes and the means of processing of personal data. |
| 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

The schools in the Warriner Multi Academy Trust process personal data relating to parents, pupils, staff, governors, visitors and others, and therefore are data controllers.

The schools are registered as data controllers with 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 the Warriner Multi Academy Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Directors board

The Directors' Board has overall responsibility for ensuring that all schools in the WMAT comply with all relevant data protection obligations. The responsibility for monitoring this will be delegated to the Local Governing Bodies of each school.

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 Directors' 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.

They are also responsible for;

Reporting Data breaches to the ICO

Ensuring Data is owned and processed across the WMAT according to our own policies and procedures.

Disseminating guidance and advice to all schools in the WMAT.

Be the first point of contact for all staff with Data Protection queries as outlined in 5.5

To process Subject Access Requests

To undertake data audits

Our DPO is Julia Jackman and is contactable on j.jackman@warriner.oxon.sch.uk

5.3 Headteacher

The Head Teacher 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 WMAT [Data-ChampionDPO](#) 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 school 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 the school 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 [2016](#) and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

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 schedule in appendix 2.

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 or students at risk
- We need to liaise with other agencies – we will seek consent ~~if as an~~ 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 or email to the Data Protection Officer; Julia Jackman, The Warriner School, Bloxham. OX15 4LJ | j.jackman@warriner.oxon.sch.uk

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, Julia Jackman.

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 13 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 primary schools 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.

Children aged 13 and above are generally 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 secondary schools may not 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 DPC. If staff receive such a request, they must immediately forward it to the DPC.

10. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash) we will comply with the requirements of the [Protection of Freedoms Act 2012](#).

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it. [If either parent refuses, this overrules one parent's consent and consent is deemed to have been refused.](#)

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners using a code issued to them.

Parents/carers and pupils from the age of 13, can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

Where there is a discrepancy on consent between parents/carers ie- one party has objected or withdrawn consent, we will not process that data irrespective of any consent given by another parent/carer.

As required by law, if a pupil from the age of 13 refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

11. CCTV

We use CCTV in various locations around the WMAT school sites to ensure they remain 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 Nichola Gardner, Business Director.

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school. Some photographs and/or recorded images form part of the child's educational record, for which we do not need to obtain parental consent.

For other uses of photographs, we will obtain written consent from at least one parent/carer 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 school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Parents/carers and pupils from the age of 13, can refuse or withdraw consent, at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

Where there is a discrepancy on consent between parents/carers ie- one party has objected or withdrawn consent, we will not process that data irrespective of any consent given by another parent/carer.

As required by law, if a pupil from the age of 13 withdraws consent, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

We will not use, or allow the use of, children's names in any images accessed externally to the school (for example social media, other websites or newspapers) without seeking your express consent

13. 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

14. 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
- Working towards a position where 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
- 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)

15. 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.

16. Personal data breaches

Our schools 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 a school laptop containing non-encrypted personal data about pupils

17. Training

All staff and governors are provided with data protection training as part of their induction process [and ongoing refresher training](#).

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

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the Directors Board.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme

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 DPC
- The DPC will liaise with the DPO to 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.
- 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.
- 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)
- The DPO/DPC and 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

APPENDIX 2 – PRIVACY NOTICES

Privacy notice for pupils within The Warriner MAT

You have a legal right to be informed about how our school uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This privacy notice explains how we collect, store and use personal data about you. We, The Warriner Multi Academy Trust, are the 'data controller' for the purposes of data protection law.

Our data protection officer is Julia Jackman. She can be contacted at j.jackman@warriner.oxon.sch.uk or on 01295 720777 (during term time).

The personal data we hold

We hold some personal information about you to make sure we can help you learn and look after you at school.

For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.

This information includes but is not limited to:

- Your contact details
- Your test results
- Your attendance records
- Your characteristics, like your ethnic background or any special educational needs
- Any medical conditions you have including any relating to COVID19
- Details of any behaviour issues or exclusions
- Photographs
- CCTV images

Why we use this data

We use this data to help run the school, including to:

- Get in touch with you and your parents when we need to
- Support your learning
- Provide appropriate pastoral care
- Check how you're doing in exams and work out whether you or your teachers need any extra help
- Track how well the school as a whole is performing
- Look after your wellbeing
- Support your transition to your next provider of education
- Support the NHS Test and Trace system where relevant to the Covid 19 pandemic

Our legal basis for using this data

We will only collect and use your information when the law allows us to. The main pieces of legislation we comply with are:-

General Data Protection Act (2016) Article 6 1 (c) (*processing is necessary for compliance with a legal obligation to which the controller is subject*)

General Data Protection Act (2016) Article 9, 2 (b) (*processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law*)

The Education (Information About Individual Pupils) (England) Regulations 2013, section 3

The Education Act (1996)

Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use your personal information where:

- You, or your parents/carers have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interest)

Where we have got permission to use your data, you or your parents/carers may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent.

Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

Collecting this information

While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.

We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

How we store this data

We will keep personal information about you while you are a pupil at our school. We may also keep it after you have left the school, where we are required to by law.

Data retention

Data is retained in-line with our Data Protection Policy and Retention Schedule which can be obtained via our website.

Data sharing

We do not share personal information about you with anyone outside the school without permission from you or your parents/carers, unless the law and our policies allow us to do so.

Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- *Our local authority – to meet our legal duties to share certain information with it, such as concerns about pupils' safety and exclusions*
- *The Department for Education (a government department) – to meet our legal obligation*
- *Your family and representatives – we may have information about any family circumstances that may affect your welfare or happiness*
- *Educators and examining bodies*

- *Our regulator (the organisation or “watchdog” that supervises us), OFSTED*
- *Suppliers and service providers – so that they can provide the services we have contracted them for under our strict data protection guidelines.*
- *Central and local government – to meet our legal obligation*
- *Survey and research organisations – only if the research is linked to local authority, central government or Department of Education.*
- *Health authorities – such as NHS England to share information about your child’s health and wellbeing*
- *Health and social welfare organisations – School Nurse, Hospital Schools, Social services, Local Authority and Department of Education.*
- *Professional advisers and consultants – Regulated companies who attend school to deliver bespoke training to students whose own company meet our strict data protection policy.*
- *Charities and voluntary organisations – Counsellors and Mentors as required*
- *Police forces, courts, tribunals – to meet our legal obligation*
- *Professional bodies*

National Pupil Database

We are required to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.

Some of this information is then stored in the [National Pupil Database](#), which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research.

The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations which promote children’s education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

You can find more information about this on the Department for Education’s webpage on [how it collects and shares research data](#).

You can also [contact the Department for Education](#) if you have any questions about the database.

Youth support services

Once you reach the age of 13, we are legally required to pass on certain information about you to Oxfordshire County Council as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Your parents/carers, or you once you’re 16, can contact our data protection officer to ask us to only pass your name, address and date of birth to Oxfordshire County Council.

Transferring data internationally

We do not transfer data to countries outside of the United Kingdom.

How to access personal information we hold about you

You can find out if we hold any personal information about you, and how we use it, by making a '**subject access request**', as long as we judge that you can properly understand your rights and what they mean.

For The Warriner students, an exception to this is for Summer 2020 **Centre Assessment Grades and Rankings**; you may request this specific data and we will provide it as soon as possible (and within a maximum of 5 working days), either electronically or on paper. You must request this, not your parent or carer, and it will be released solely to you. This request will be dealt with by our Data Protection Officer or another member of staff in her absence and logged accordingly.

You may also ask us to send your personal information to another organisation electronically in certain circumstances.

You may have other rights over how your personal data is used and kept safe, including the right to:

- Say that you don't want it to be used if this would cause, or is causing, harm or distress
- Stop it being used to send you marketing materials
- Say that you don't want it used to make automated decisions (decisions made by a computer or machine, rather than by a person)
- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- Claim compensation if the data protection rules are broken and this harms you in some way

If you want to make a request please contact our data protection officer.

Complaints

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong. You can make a complaint at any time by contacting our data protection officer.

You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

Julia Jackman
The Warriner School
Bloxham
OX15 4LJ

j.jackman@warriner.oxon.sch.uk

This notice is based on the [Department for Education's model privacy notice](#) for pupils, amended to reflect the way we use data in this school.

Privacy notice for parents/carers/guardians

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils**.

We, The Warriner Multi Academy Trust, are the 'data controller' for the purposes of data protection law.

Our data protection officer is Julia Jackman.

The personal data we hold

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

- Contact details, contact preferences, address/addresses of parents, date of birth, identification documents, gender, previous school history, transport information.
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health including any relating to COVID19
-
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data 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

- Carry out research
- Comply with the law regarding data sharing
- Support the NHS Test and Trace system where relevant to the Covid 19 pandemic

Our legal basis for using this data

We only collect and use pupils' personal data when the law allows us to. The main pieces of legislation we comply with are:-

General Data Protection Act (2016) Article 6 1 (c) (*processing is necessary for compliance with a legal obligation to which the controller is subject*)

General Data Protection Act (2016) Article 9, 2 (b) (*processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law*)

The Education (Information About Individual Pupils) (England) Regulations 2013, section 3

The Education Act (1996)

Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations.

Data retention

Data is retained in-line with our Data Protection Policy and Retention Schedule which can be obtained via our website.

Data sharing

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

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- *Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns, grades and exclusions*
- *The Department for Education – to meet our legal obligations to share certain information with it, such as safeguarding concerns, grades and exclusions*
- *The pupil's family and representatives – we may have information about any family circumstances that may affect your child's welfare or happiness*
- *Educators and examining bodies*
- *Our regulator Ofsted for inspection and regulation (pertaining to our students)*
- *Suppliers and service providers – to enable them to provide the service we have contracted them for*
- *Central and local government – only in the instance that meets any legal obligations*
- *Survey and research organizations – only if the research is linked to our local authority, central government or the Department of Education.*
- *Health authorities – such as NHS England to share information about your child's health and wellbeing*
- *Health and social welfare organisation's – School Nurse, Hospitals schools, Social services, Our Local Authority, Department of Education*
- *Professional advisers and consultants – Regulated companies who attend school to deliver bespoke training to students whose own company meets strict data protection policy*
- *Charities and voluntary organisations – Counsellors and Mentors*
- *Police forces, courts, tribunals – to meet legal obligations*
- *Professional bodies*

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school 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 database is held electronically so it can easily be turned into statistics. 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 other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on [how it collects and shares research data](#).

You can also [contact the Department for Education](#) with any further questions about the NPD.

Youth support services

Once our pupils reach the age of 13, we are legally required to pass on certain information about them to Oxfordshire County Council, as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Parents/carers, or pupils once aged 16 or over, can contact our data protection officer to request that we only pass the individual's name, address and date of birth to Oxfordshire County Council.

Transferring data internationally

We do not transfer data to countries outside of the United Kingdom.

Parents and pupils' rights regarding personal data

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

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

If you would like to make a request please contact our data protection officer.

Complaints

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong. You can make a complaint at any time by contacting our data protection officer.

You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

Jula Jackman
The Warriner School
Bloxham
OX15 4

This notice is based on the [Department for Education's model privacy notice](#) for pupils, amended to reflect the way we use data in this school.

Privacy notice for staff within The Warriner MAT

Privacy Notice – General Data Protection Regulations (GDPR) 2016 and Data Protection Act (2018)

The Warriner MAT is a data controller for the purposes of the GDPR/DPA. We can be contacted as follows:-

| | | |
|---------------------|-------|--|
| The Warriner MAT | Tel | 01295 720777 |
| The Warriner School | Email | j.jackman@warriner.oxon.sch.uk |
| Bloxham | | |
| OX15 4LJ | | |

Our Data Protection Officer is Julia Jackman. She can be contacted via the details above.

Collecting school workforce information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order 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. We hold school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the DFE and Local Authority for their statistical returns
- inform the development of recruitment and retention policies
- enable individuals to be paid

This data includes personal information (such as name, employee or 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 information), work absence information (such as number of absences and reasons), qualifications (and, where relevant, subjects taught), medical information, addresses, bank details, next of kin contact details, references, documentation to enable the DBS application process to be completed

This data may only be used or shared for specific purposes allowed by law to organisations like:-

| | |
|---|---|
| Local Authorities and their contractors | Department for Education (DfE) and their contractors |
| Payroll and personnel (Selima/ Access People) | Approved third party software providers |
| Occupational Health | NHS Test and Trace system where relevant to the Covid 19 pandemic |

All these are data controllers in respect of the data they receive and are subject to the same legal constraints by law in how they deal with the data.

We collect the majority of this data under contractual and legal obligations. We also collect data that you have given your consent for us to hold/use (eg photograph) that protects your interests (eg health information or employer references) and for public interest (eg for statutory purposes)

The lawful basis on which we use this information

We collect and use workforce information under our legal obligation and relevant policies. The main pieces of legislation we comply with are:-

Section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments - we are required to share information about our workforce members with our local authority (LA) and the Department for Education (DFE)

General Data Protection Act (2016) Article 6 1 (c) *(processing is necessary for compliance with a legal obligation to which the controller is subject)*

General Data Protection Act (2016) Article 9, 2 (b) *(processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law)*

Why we share workforce information

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

The 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 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 department 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 department 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 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 department's data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

To contact the department: <https://www.gov.uk/contact-dfe>

We do not transfer data to countries outside of the United Kingdom.

Data retention

Data is retained in-line with our Data Protection Policy and Retention Schedule which can be obtained via our website <https://www.thewarrinerschool.co.uk/attachments/download.asp?file=1213&type=pdf> or a paper copy can be provided on request.

Requesting access to your personal data

You have the right to request a copy of the information that we hold about you (known as a Subject Access Request), to request that inaccuracies are rectified and to request the deletion of personal information. Please contact our Data Protection Officer in writing for more information.

If you would like to discuss anything in this privacy notice or make a complaint about our data procedures, please contact our Data Protection Officer in the first instance (see contact details on page 1).

If you wish to escalate a complaint, please contact the Information Commissioner's Office <https://ico.org.uk/> or 0303 123 1113.

Privacy Notice – Coronavirus – NHS Test and Trace – The Warriner MAT

The development of the NHS 'Test and Trace' scheme is a key part of the government plan to manage Coronavirus.

As we respond to Government guidance and the wider opening of schools, the safety and well-being of pupils, staff and their families is a priority. Plans to manage a safe return are in place, however our responsibility extends beyond the school gates.

We hold a lot of data and, as part of our statutory duty, it *may* be necessary for us to share that data on request by Public Health with NHS Test and Trace workers, so that we play our part in making the programme as effective as possible.

It is likely that we will be asked to provide contact details if a case of Coronavirus or a suspected case arises in our Trust/school. There is an obligation to support Government planning and we will provide details if requested to do so. We will be sharing data on the basis that this is a Public Duty (see below) and that, in the case of any health data, it is necessary for the public interest, as set out.

Our first response will be to try to make contact with individuals directly ourselves to manage information and sharing data. However, in some cases we may be required to provide it to the new service.

Please be assured that we will keep a record of information that we share.

This Privacy Notice should be read in alongside the other GDPR and Data Protection on our website.

NHS Test and Trace and the law

The law on protecting personally identifiable information, known as the General Data Protection Regulation (GDPR), allows Public Health England to use the personal information collected by NHS Test and Trace.

The section of the GDPR that applies is:

Article 6(1)(e) 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'

As information about health is a special category of personal information, a further section of the GDPR applies:

Article 9(2)(i) 'processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare'

Public Health England also has special permission from the Secretary of State for Health and Social Care to use personally identifiable information without people's consent where this is in the public interest. This is known as 'Section 251' approval and includes the use of the information collected by NHS Test and Trace to help protect the public from coronavirus. The part of the law that applies here is Section 251 of the National Health Service Act 2006 and the associated Health Service (Control of Patient Information) Regulations 2002.

Rights of Employees/Pupils/Students/Children/Visitors in relation to their personal data

All our employees/pupils/students/children/visitors have the right to request access to personal data that we hold about them. To make a request for access to their personal data, individuals should contact our Data Protection Officer, Julia Jackman at j.jackman@warriner.oxon.sch.uk

Please also refer to our Data Protection Policy for further details on making requests for access to personal data.

Individuals also have the right, in certain circumstances, to:

- Object to the processing of their personal data
- Have inaccurate or incomplete personal data about them rectified
- Restrict processing of their personal data
- Object to the making of decisions about them taken by automated means
- Have your data transferred to another organisation
- Claim compensation for damage caused by a breach of their data protection rights

If an individual wants to exercise any of these rights then they should contact Data Protection Officer, Julia Jackman at j.jackman@warriner.oxon.sch.uk

The law does not oblige the Trust/school to comply with all requests. If the Trust/school does not intend to comply with the request, then the individual will be notified of the reasons why in writing.

Concerns

If an individual has any concerns about how we are using their personal data, then we ask that they contact our Data Protection Officer in the first instance. However an individual can contact the Information Commissioner's Office should they consider this to be necessary, at <https://ico.org.uk/concerns/>.

Privacy notice for Members, Trustees, Governors and other volunteers

Under data protection law, individuals have a right to be informed about how the Trust or school uses any personal data we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals working with the Trust or any of our schools in a voluntary capacity, including Governors and Trustees.

We, The Warriner Multi Academy Trust are the 'data controller' for the purposes of data protection law.

Our data protection officer is Julia Jackman. She can be contacted at j.jackman@warriner.oxon.sch.uk or on 01295 720777 (during term time).

The personal data we hold

We process data relating to those volunteering at our Trust. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth
- References
- Evidence of qualifications
- Employment details
- Information about business and pecuniary interests

We may also collect, store and use information about you that falls into “special categories” of more sensitive personal data. This may include information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Disability and access requirements

Why we use this data

The purpose of processing this data is to support the Trust to:

- Establish and maintain effective governance
- Meet statutory obligations for publishing and sharing Governors and Trustees details
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Undertake equalities monitoring
- Ensure that appropriate access arrangements can be provided for volunteers who require them

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else’s interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify our use of your data.

Collecting this information

While the majority of the information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

Personal data is stored in accordance with our data protection policy

We maintain a file to store personal information about all volunteers. The information contained in this file is kept secure and is only used for purposes directly relevant to your work with the Trust.

When your relationship with the Trust has ended, we will retain and dispose of your personal information in accordance with the Information and Records Management Society's toolkit for schools. (Guidance on the retention of governor records begins on page 37.)

Data sharing

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

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Government departments or agencies – to meet our legal obligations to share information about governors/trustees
- Our local authority – to meet our legal obligations to share certain information with it, such as details of governors.
- In our Church schools the Oxfordshire Diocesan Board of Education – to enable them to provide support to our Governance teams.
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as governor/trustee support
- Police forces, courts – to meet our legal obligations

Transferring data internationally

We do not transfer data to countries outside of the United Kingdom.

Your rights

How to access the personal information we hold about you

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have a right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113

- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

Julia Jackman
The Warriner School
Bloxham
OX15 4LJ

j.jackman@warriner.oxon.sch.uk