

Owlcotes Multi-Academy Trust

General Data Protection Regulation – Data Protection Policy



October 2019

Last Reviewed: March 2023

Contents

1.	Introduction	3
2.	Principles.....	4
3.	Roles and Responsibilities	4
4.	Data Audit.....	5
5.	Processing Records	5
6.	Sharing Data.....	6
7.	Owlcotes Multi-Academy Trust Specific Data Security Measures – Data Protection by Design.....	6
8.	Data Breaches.....	7
9.	Training.....	7
10.	Data Protection Impact Assessment	7
11.	Right to Access Information	7
12.	Right to Erasure	8
13.	Monitoring.....	8

About Owlcotes Multi-Academy Trust

OMAT is committed to the development of inclusive schools, sharing a common purpose to provide excellent education and improved outcomes for pupils.

OMAT strives to provide high-quality education for all children within our local communities by inspiring innovation, creativity and aspiration through an enriched curriculum.

OMAT is committed to the principles of co-operation, collaboration and sharing best practice with a strong focus on staff development.

OMAT is also committed to the preservation of the unique identity of all schools within the trust: each school will have a Local Governing Board (LGB) that is involved in decision making at school level, with autonomy to make decisions for its own school in line with the Scheme of Delegation.

All Trustees and any schools joining must agree to share and uphold all of these principles now and in the future.

1. Introduction

Owlcotes Multi-Academy Trust and its schools will need to collect and store information about its staff, pupils, and other stakeholders for the purposes of safeguarding and personnel records.

This Data Protection Policy has been produced with due regard to the following legislation:

- The Data Protection Act 2018;
- The General Data Protection Regulations 2018;
- The Freedom of Information Act 2000;
- The Education (Pupil Information) (England) Regulations 2005;
- ICO General Data Protection Regulation (GDPR) 2018.

This list is not exhaustive and multiple resources were used to produce this Data Protection Policy.

This Policy will be implemented alongside school policies such as:

- Freedom of Information Policy;
- E-Safety Policy;
- Acceptable Use of ICT Policy;
- Use of Data Privacy Notices.

Members of staff will gain familiarisation with the requirements of the GDPR by consulting this policy, the school policies above.

The Trust collects and processes personal data about pupils, staff, governors and other Trust users in order to fulfil its statutory and administrative functions and duties.

The Trust is a Data Controller as it processes data that is the personal information of pupils, families, staff, visitors and other Trust users.

The Trust is a Data Processor as it processes data on behalf of other public bodies such as the DfE.

Principles

- Personal data must be processed lawfully, fairly and transparently;
- Personal data can only be collected for specific, explicit and legitimate purposes;
- Personal data must be adequate, relevant and limited to what is necessary for processing;
- Personal data must be accurate and kept up-to-date;
- Personal data may identify the data subject only as long as is necessary for processing;
- Personal data must be processed in a manner that ensures its security;
- Any breaches in data security must be reported to the ICO within 72 hours;
- The Trust must report any breaches caused by third parties who have access to Trust users' data within 72 hours;
- The Trust must inform any data subject (person identified in data) where a data breach may have led to the unauthorised access to their personal information.

2. Roles and Responsibilities

The Trust's privacy statements set out in detail how the Trust will maintain the security of Trust users' data. The Acceptable Use Policies set out the duties of the staff and other Trust users in supporting data security.

Owlcotes Multi-Academy Trust CEO, school Headteachers, and school Senior Leadership Teams are responsible for ensuring that the requirements of GDPR are upheld and ensuring that all members of staff who manage and process personal data understand that they are responsible for following good data protection practice.

In addition to the obligations set out in this policy, all Owlcotes Multi-Academy Trust employees are responsible for:

- Maintaining confidentiality and adhering to data protection legislation;
- Ensuring that any information they provide to the Trust in relation to their employment is accurate;
- Informing the Trust or school office of any changes to information which they have previously provided (e.g. change of home address);
- Where required, verifying the accuracy of any information previously provided;
- Informing the Trust of any errors in the information previously provided. The Trust or its schools cannot be held responsible for errors in information provided by an employee.

If employees, as part of their responsibilities, collect information about other individuals, then these employees must comply with the provision of this Policy.

Within the Trust the security of data is coordinated by Joe Wilson.

The Trustee with special responsibility for data security is John Woods.

The Trust has appointed a **Data Protection Officer** who has responsibility for overseeing the implementation of this policy and all GDPR related documents. The DPO will monitor compliance, report to the Trust leadership and support the Trust with updates and interpretations as the GDPR develops.

The DPO will liaise between the Trust and the ICO and must be informed as soon as is practicable of any personal data security breach.

The DPO will support the Trust in its communication with Trusts users (pupils, families, parents, governors, contractors and visitors) about the Trust's GDPR procedures. This will include the drafting of privacy statements, acceptable use policies and data subjects rights.

Data subject requests should be made in writing to the relevant school's Officer Manager, or the OMAT Head of Communication and Information. The DPO might have to respond to any or all of the following:

- Why the data is processed;
- On which basis;
- Who has seen it;
- How long it will be stored for;
- Where the data was sourced;
- Whether decisions have been based on the data.

Children below the age of 13 do not have the right to make a subject access request, so requests must be made by parents. The Trust may take into account the views of a pupil.

The Trust's Data Protection Officer is Mr Joe Wilson

Email: info@owlcotesmat.org

Tel: 0113 8874523

The DPO's duties are set out in detail in the service level agreement and contract held between the Trust and Fusion Education People Solutions. Staff should contact the DPO should they believe that this policy and/or the privacy statements and/or the acceptable use policies are not being followed.

3. Data Audit

The Trust will carry out a data audit with support from Fusion Education People Solutions and their technical support company. Within the audit the Trust will record all third parties' compliance with the GDPR if those third parties process data for any Trust users. Such confirmation will, from now on, be an essential part of any contract with third parties when the processing of Trust users' data is involved. The Trust will not share data, or have any data processed, by any third parties who do not confirm their compliance with GDPR requirements.

The audit will also check the security of physical and digital records and devices.

4. Processing Records

To meet the ICO's recommendation that 'scrupulous records' are developed the Trust will record its processing of data and the results of its data audit. It will record the ongoing security measures for physical and digital filing systems. Confirmation of compliance by third parties accessing any Trust user data will be recorded.

In broad terms, the Trust will record which data has been processed (including deletions when data should no longer be stored) on which legal basis. Consent replies are recorded within the system.

5. Sharing Data

Personal data may be shared with third parties to:

- Protect the vital interests of a child;
- Protect the vital interests of a member of staff;
- To prevent or support the detection of fraud or other legal proceedings;
- When required to do so by HMRC.

CCTV

CCTV is used to support the safety and security of Trust users. We adhere to the ICO's code of practice* for its use. Although consent is not required for its use prominent notices inform Trust users that CCTV is used within the Trust site.

**In the picture: A data protection code of practice for surveillance cameras and personal information.*

Photographs and Moving Images

Consent is requested from parents and staff for the use of images. Letters requesting consent outline the choices that pupils and staff may make for the use of their images.

The Trust may seek consent to use photographs for the following purposes:

- To support Trust user welfare (identity and security);
- To celebrate achievement within the classroom;
- To celebrate achievement within the Trust;
- To celebrate achievement in the printed press;
- To celebrate achievement online.

6. Owlcotes Multi-Academy Trust Specific Data Security Measures – Data Protection by Design

- a) All IT systems - mobile devices, laptops, tablets, mobile phones and any device capable of processing data, will be password protected.
- b) All IT systems will be kept securely; the server and hard disks will be in a locked cabinet and the server room locked when the Trust is closed and at other times of reduced security; desktop computers and portable devices will be sited/stored in secure places.
- c) Staff are expected to ensure the safety of their allocated Trust devices: devices may not be left unattended in cars at any time and they must be kept out of sight if taken home.
- d) All passwords must be 'strong;' (at least 8 characters with a mixture of upper and lower case letters, numbers and symbols), the Trust will require regular changing of passwords.
- e) No passwords will be written down or shared; advice is available on the safe storage of passwords.
- f) The Trust will devise granulated levels of access as appropriate to staff responsibilities for access to personal data.
- g) Devices that are used to process sensitive data and/or are vulnerable to theft will be secured with encryption.
- h) All emails containing personal data will use Trust systems and be encrypted.
- i) All deleted data will be deleted in a secure manner: physical data will be shredded and digital data will fully deleted with trash / junk emptied regularly. Hard disks no longer required will have the data on them deleted and the deletion certified by an external data support company.

- j) Only data that is necessary for the effective performance of the Trust will be processed.
- k) Data protection will be integrated into all appropriate policies and procedures (e.g. staff induction).
- l) Staff will be updated with any significant interpretations or developments of the GDPR.
- m) The Trust will have data impact assessments in place to protect vulnerable data subjects and sensitive data.
- n) Data contained within an email, or attached to an email, will be transferred to a secure folder and the email deleted.
- o) Physical data will be kept securely, having regard to the sensitivity of the data and the vulnerability of the data subject e.g. medical data will be accessible to those who need to support a Trust user's needs, but not to others.
- p) All Trust users will handle personal data with care: it will not be left unattended (unattended computers must be locked), Trust users will not allow others to oversee personal data (screens must be positioned with care); papers must not be left where others can see them.
- q) All computers that might be used to process data will be set to lock (a screensaver will activate) after a period of inactivity.
- r) School Headteacher and/or the DPO will approve who and how personal data is stored on mobile devices.
- s) All digital data that is stored will be backed up on at least password protected devices.
- t) Personally owned devices will not be used for the storage of Trust personal data.

7. Data Breaches

All staff must report to the Headteacher or a member of the SLT any suspected data breaches (the loss, theft, unauthorised access to data, including the accidental sharing of personal data via a wrongly addressed email etc.) immediately. It will be for the Headteacher or SLT to decide whether to the suspected data breach warrants reporting to the Data Protection Officer or the ICO. If reported to the DPO, it will be for them to decide whether to report the suspected data breach to the ICO.

8. Training

All staff will receive basic training in the requirements of the GDPR. The training will be recorded in the data audit and/or the data processing records. Governors will also receive a briefing. Data protection will form a part of pupils' e-safety education. The Trust will keep staff and governors up to date with guidance, changes and interpretations to data protection law.

9. Data Protection Impact Assessment

For the Trust's most sensitive data processing activities the Trust will have completed a DPIA to ensure that the risk to individuals of a data breach is minimised, as should be the risk to the Trust's reputation. Staff involved in processing the Trust's most sensitive data will have to record their reading and understanding of the relevant DPIA.

10. Right to Access Information

Any individual whose personal data is stored by Owlcotes Multi-Academy Trust and its schools has the right (subject to certain statutory exemptions and restrictions) to access any personal data that is held about them.

Any individual who wishes to exercise this right should submit the request in writing. Such requests should be immediately referred to Owlcotes Multi-Academy Trust's DPO.

All requests will be responded to within a period of month after receipt. Owlcotes hold the right to refuse a request.

Owlcotes Multi-Academy Trust will verify the identity of the individual making the requests before any information can be supplied.

All requests will be responded to within 30 days of receipt. If the request is for numerous pieces of data, or a complex request, the period of response will be extended by a further 60 days. The individual making the request will be informed of the extended response time and the reason behind it.

Owlcotes Multi-Academy Trust holds the right to refuse to respond to a request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority.

A proforma for a subject access request for personal data can be found in Appendix 1.

11. Right to Erasure

Individuals whose personal data is stored by Owlcotes Multi-Academy Trust have the right to request deletion or removal of personal data if there is no compelling reason for its continued storage.

Individuals hold the right to request erasure in the following circumstances:

- The personal data stored is no longer necessary in relation for the purpose for which it was originally collected;
- If the individuals objects to the processing of their personal data and there is no legal interest for continuing processing;
- The personal data was incorrectly or unlawfully processed;
- The personal data is required to be erased in order to comply with a legal obligation;

Owlcotes Multi-Academy Trust has the right to refuse a request for data erasure where the personal data is being processed for the following reasons:

- To comply with a freedom of information request;
- To comply with a legal obligation for the performance of a public interest task or request of official authority;
- For public health purposes in the public interest;
- The exercise or defence of legal claims.

12. Monitoring

The DPO will lead the formal monitoring of the Trust's compliance with the GDPR. Every member of staff and governor shares a responsibility to monitor compliance and to report any suspected failures to comply.

Footnotes

Data subjects' rights include:

- The right to be informed;
- The right of access;
- The right to object;
- The right to be forgotten (this might prove impossible in the Trust context);
- The right of rectification (any inaccurate data must be corrected).

In deciding whether to pass on a suspected data breach to the ICO the DPO will consider whether the data breach might affect a person's:

- Reputation;
- Confidentiality;
- Financial wellbeing;
- A loss of control over their data;
- Make them vulnerable to discrimination;
- Their rights and freedoms.

Definitions

Data processing: The acquisition, storage, processing and transmission of data.

Data subject: Any identifiable person whose data is processed.

Consent: Must be freely given, specific and an unambiguous indication of the subject's wishes. It must be recorded and available to an audit. A person must be 13 years old in order to record their consent.

Cross-border processing: The GDPR covers all EU states and will remain part of UK law. Data cannot be stored beyond the EU and UK borders (the exact borders are those of the European Economic Area).

Sensitive data: The GDPR/ICO requires that particular care is taken with the following data:

- Data regarding children;
- Health (physical, mental, genetic);
- Ethnicity;
- Religion;
- Sexuality;
- Performance management and trade union membership.

Filing system: Any structured set of personal data, however stored in any format (physical or digital) that can be processed.

Personal data breach: A breach of data security leading to the accidental or unlawful destruction, loss, theft, alteration, unauthorised disclosure, destruction, sale or access to any processed data.

Data subjects affected by a data breach must be informed of the breach within 72 hours. Breaches must be reported to the ICO within 72 hours.

Pseudonymisation: The act of making data anonymous. There must be security between pseudonymised data and any data that could re-identify a person.

Password protection: The act of 'locking' a device or document. The information remains readable beyond the password.

Encryption: The act of encoding all the information beyond a password or code.

Legal basis: The Trust decides, and registers with the ICO, upon which legal basis it processes data. As a public body with set duties, the Trust uses the following bases for processing and controlling data.

Legal basis: **Public Task:**

- Admissions;
- Attendance;
- Assessment;
- Pupil and staff welfare;
- Safe recruitment;
- Staff training.
- Performance Management.

Legal basis: **Consent:**

- Various uses of photographs and moving images;
- Trade union membership;
- Staff ethnicity, religion and health data (Note the Staff Privacy Statement);
- The use of data to promote the social life of the Trust community.

Legal basis: **Contract:**

- When processing is required to carry out the performance of a contract.

Personal data: Anything that might lead to the identification of a person: name, number, characteristics, photograph, correspondence.

Data portability, data subject access request: Data subjects (or a child's parents) may request access to a copy of all their data. The Trust has established an efficient means of accomplishing this task that may not carry a charge and will be completed within 15 working days. Data subjects may request that data is brought up-to-date or made more accurate.

Appendix 1: Subject Access Request Form

Owlcotes Multi-Academy Trust and its schools need to collect and store information about its staff, pupils, and other stakeholders for the purposes of safeguarding and personnel records.

Information is collected and stored in accordance with the following legislation:

- Data Protection Act 2018;
- General Data Protection Regulations 2018;
- Freedom of Information Act 2000;
- Education (Pupil Information) (England) Regulations 2005;
- ICO General Data Protection Regulation (GDPR) 2018.

This list is not exhaustive.

Any individual whose personal data is stored by Owlcotes Multi-Academy Trust and its schools has the right (subject to certain statutory exemptions and restrictions) to access any personal data that is held about them.

Any individual who wishes to exercise this right should submit the request in writing. Such requests should be immediately referred to the appropriate school's Office Manager or to the Owlcotes Chief Information Office. More complex requests may be referred to Owlcotes Multi-Academy Trust's Data Protection Officer.

Owlcotes Multi-Academy Trust schools will verify the identity of the individual making the requests before any information can be supplied.

All requests will be responded to within one month of receipt. If the request is for numerous pieces of data, or a complex request, the period of response will be extended by a further month. The individual making the request will be informed of the extended response time and the reason behind it.

Owlcotes Multi-Academy Trust holds the right to refuse to respond to a request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority.

Children below the age of 13 do not have the right to make a subject access request, so requests must be made by a parent/carer. The Trust may take into account the views of a pupil.

Please note, information released as part of a subject access request may contain redacted information about other individuals who have not given their consent for their personal data to be released. If information released in response to a subject access request contains information about other individuals who are not the subject of the request, the school or Trust does not have an obligation to request permission to release the data of individuals who are not the subject of the request itself.

Subject Access Request Form

Dear Headteacher,

Please can you provide me with the information specified below about (name) _____ that I am entitled to request under the General Data Protection Regulations 2018 and Freedom of Information Act 2000.

Please complete the information below:

Name of School:	
Name of Person Requesting Information:	
Child's Name (if applicable):	
Please specify the nature of your relationship with the school (please delete as appropriate):	<ul style="list-style-type: none"> • Parent/carer • Pupil • Employee • Visitor • Governor • Other (please specify):
Correspondence Address:	
Contact Telephone Number:	
Email Address:	
Nature of the information requested: <i>Please insert details here of the information that you would like to request. Please be as precise as possible in order to help the school locate the specific information. For example:</i> <ul style="list-style-type: none"> • <i>My employee personnel file</i> • <i>My child's medical records</i> • <i>My child's behaviour records</i> 	

The school may contact you if any further information is required, or to inform you regarding the status of your request.

FOR SCHOOL OFFICE USE ONLY:

Date request received:		
Identity verified:	I.D. verified date:	I.D. verifier's initials:
Date passed to Headteacher:		
Date passed to DPO (if applicable):		
School contact for subject access request:		
Request acknowledged:		
Request replied:		

**This Data Protection Policy was adopted by Owlcotes Multi Academy Trust on
31/10/2019**

Chair of Trustees: Mrs Judith Norfolk		
Signature:		Judith Norfolk
Frequency of review:	2 years	
To be reviewed by:	FRAC	
To be approved by:	OMAT Full Board	
Date of next review:	March 2025	

REVIEW RECORD

Date of review	Reason for review	Date of next review
11/02/2021	Addition of sections 11 and 12 and more information added to sections 1 and 3.	Feb 2023

Name:		Signature:	
-------	--	------------	--

on behalf of OMAT Full Board

Date of review	Reason for review	Date of next review
23/03/2023	Updated DPO contact details, amendments to section 7 and 10 and addition of Appendix 1.	March 2025

Name:		Signature:	
-------	--	------------	--

on behalf of OMAT Full Board

Date of review	Reason for review	Date of next review

Name:		Signature:	
-------	--	------------	--

on behalf of OMAT Full Board