Omnia
LEARNING TRUST

Data Protection Policy

Contents

Policy Review Schedule

Policy	OLT Data Protection Policy
Review schedule	Annual (unless changes in guidance and legislation require an immediate update)
Statutory Policy	Yes
Policy owner	CEO
Lead Reviewer	HOO (external check when there is a change in legislation)
Approver and date of last approval	OLT Operations Committee, 07/10/2025
Key review dates	**Changes made**
April 2018	Written
March 2020	Added directions for Governor/Director training
April 2020	Changes: Added E-Security Policy – deleted separate E-Security Policy Amended training section Added Data Deletion Day Added GDPR team meetings and remits Added list of related policies and documents Added use of GDPRIS and IRMS (Data Retention Schedule) Revised information on Data Asset Registers

	Revised information on Subject Access Requests Updated role of DPO Added clarity on keeping pupil data when a pupil has left Updated information on consent for pupil photos
April 2021	Changes: Removed links to EU legislation and replaced with a reference to "UK data protection law" Added reference to UK GDPR legislation Updated wording on the transfer of personal data outside the UK (legislation no longer covers EEA) Replaced GDPR with UK GDPR Data protection law wording updated to UK data protection law Review frequency is now annual in line with DfE recommendation on statutory policies
April 2022	CCTV section updated to reflect ICO changes
September 2022	Reference added to mandatory Cyber Security training (RPA Scheme requirement)
September 2023	Reference added to the new web filtering and monitoring requirements required by KCSIE 2023 Reference to GDPR meetings updated (OLT Compliance report)
September 2024	Reference to external review updated "when there is a change in legislation". Reference to RPA training updated – annual mandatory cyber security training. Definitions table updated to ensure clarity Reference to GDPRIS removed, system replaced with a google form Section on AI added
October 2025	Replaced references to COO with refs to HOO/CEO as needed and updated roles and responsibilities section. Updated wording in line with Model DP Policy on The Key to include removing duplicate language. Reviewed policy in line with ICO guidance on data portability, the right to object, and on the new DUAA 2025. Removed copy of physical data breach notification form at end of policy as this process is now fully online via the ICO website. Added explicit consent form as an appendix, where it was previously a standalone document. Training section updated.
Date of next review: October 2026	

Introduction

This policy covers all the academies in the Omnia Learning Trust. It aims to ensure that data is handled correctly and sensitively for staff, pupils, parents and other key stakeholders.

Other related policies and documents – available on request

- CCTV policy – each academy has their own version.
- Document Retention Schedule.
- Freedom of Information Policy and Charging Schedule.

- Privacy notices – parents/pupils, employees, governors.
- Acceptable Use of ICT Policy and Agreement.
- GDPR Induction Checklist.
- ICT Continuity and Recovery Plan.
- Whistleblowing Policy.
- Safeguarding and Child Protection Policy – each academy has their own.
- Subject Access Request Policy
- E-Security Policy (staff).

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data, regardless of whether it is in paper or electronic format, and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Legal Framework

This policy has due regard to legislation, including, but not limited to the following:

- 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.
- The Data (Use and Access) Act 2025.
- The Freedom of Information Act 2000.
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016).
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.
- The School Standards and Framework Act 1998.
- Data Protection Act 2018 (DPA 2018).

This policy complies with our funding agreement and articles of association.

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'.
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection.
- Regulation (GDPR) 12 steps to take now'.
- The ICO's code of practice for the use of surveillance cameras and personal information.
- DfE guidance on Generative artificial intelligence in education.
- ICO guidance on the use of CCTV (surveillance cameras and personal information).

This policy will be implemented in conjunction with the Trust's Freedom of Information Policy and Charging Schedule, and its Subject Access Request Policy.

Definitions

Personal data	Information relating to identified or identifiable individuals, such as parents, children, relatives, job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. Personal data we gather may include: individuals' name, contact details, addresses, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV. Personal data may be collected from parents, staff, other schools, children, LAs, and the Department for Education.
Special categories of personal data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data is strictly controlled in accordance with this policy.
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 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

Scope

This policy applies to all staff, parents and children. Academy staff must be familiar with this policy and comply with its terms.

Roles and Responsibilities

The Trust Board
The Omnia Learning Trust Board has overall responsibility for ensuring that each school complies with all relevant data protection obligations.

The Data Controller
The Trust processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and is therefore a data controller.

The Trust is registered with the ICO and has paid its data protection fee to the ICO as legally required.

Data Protection Officer (DPO)
The DPO is responsible for overseeing the implementation of this policy and for reporting to the Trust Board about the Trust's compliance with GDPR obligations and requirements.

At September 2025, Sarah Bellingham is the named DPO for the Omnia Learning Trust. The DPO can be contacted on admin@omnialearningtrust.org. Assignment of this role is reviewed by the CEO on an annual basis.

The Data Protection Officer's responsibilities:

- Be first point of advice for key staff at each academy within the Trust; and determine how to handle and record potential breaches and subject access requests.
- Inform and advise the organisation and employees about duties and obligations to comply with the UK GDPR and other data protection laws.
- To monitor compliance with the UK GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed.
- Keep the board updated about data protection responsibilities, risks and issues.
- Review all data protection procedures and policies on a regular basis.
- Arrange data protection training and advice for all staff members and those included in this policy.
- Answering questions on data protection from parents/carers, staff, board members and other stakeholders.
- Advise academies how to respond to individuals such as clients and employees who wish to know which data is being held on them by the OLT Academies.
- Ensuring third parties that handle the company's data and any contracts or agreement regarding data processing are compliant with the UK GDPR regulations. Third parties must comply with 11 clauses of the UK GDPR regulations.
- Approving data protection statements attached to emails and other marketing copy.
- Addressing data protection queries from clients, target audiences or media outlets.
- Ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy.
- Ensure all IT systems, services, software and equipment meet acceptable security standards.
- Ensure checking and scanning security hardware and software is carried out regularly to ensure it is functioning properly.
- Researching third-party service providers, such as cloud services the company is considering using to store or process data.

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 UK

- 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

OLT Operational Compliance
The CEO and HOO compile a summary GDPR report per school on a termly basis with input from Office Managers which covers the aspects outlined in the remit below.

GDPR Remit

- DPO – trained and named.
- Staff training & induction processes undertaken
- Subject access requests completed
- Third party data handlers - DPIAs undertaken.
- GDPR legal compliance.
- Breaches – reported and remedied.
- Policy up to date
- Training requirements for Governors DPO/other key personnel up to date.
- Cybersurfing training and warnings issued to staff.
- Internal and External GDPR audits – routinely implemented
- ICT security reviewed for GDPR compliance
- IT systems reviewed for GDPR compliance

Data Processing

Fair and lawful processing
We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The processing of all data must be:

- Necessary to provide our educational environment.
- In our legitimate interests and not unduly prejudice the individual's privacy.
- In most cases this provision will apply to routine data processing activities.

Justification for personal data
We will process personal data in compliance with all eight data protection principles set out within the UK GDPR:

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
(a) at least one of the conditions in Schedule 2 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4 Personal data shall be accurate and, where necessary, kept up to date.
5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6 Personal data shall be processed in accordance with the rights of data subjects under this Act.
7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

We document any additional justification for the processing of sensitive data.

Accuracy and relevance
We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Data audit and register
Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. These will be reviewed and refreshed annually. For further details please refer to the Trust's Document Retention Schedule and its ICT Continuity and Recovery Plan.

Consent and conditions for processing data
Some data that we collect is subject to active consent by the data subject. This consent can be revoked at any time. Some data we collect is in relation to our legal responsibilities as set out in article 6 of the GDPR:

6(1)(a) Consent of the data subject.
6(1)(b) Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract.
6(1)(c) Processing is necessary for compliance with a legal obligation*.
6(1)(d) Processing is necessary to protect the vital interests of a data subject or another person.
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.
6(1) (f) Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

***Criminal record checks**

Any and all criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Privacy Notice - transparency of data protection
Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. Privacy notices for staff, parents and pupils can be found on each Academy and Trust website (also available in Parago).

The notice:

- Sets out the purposes for which we hold personal data on parents, children and employees
- Highlights that our work may require us to give information to third parties.
- Provides that our stakeholders have a right of access to the personal data that we hold about them.

Personal data
Individuals and data subjects must take reasonable steps to ensure that personal data we hold about is accurate and updated as required. For example, if personal circumstances change, please inform the relevant academy so that they can update your records.

Sharing personal data
The Trust will not normally share data with anyone else without consent but there are circumstances where we may be required to do so, including but not limited to sharing personal data with law enforcement and government bodies where legally required to do so; when there is an issue with a pupil or parent/carer that puts the safety of our staff at risk; or sharing personal data with third party organisations/service providers such as the ones listed below. If any online service is provided by the Trust or its schools for use by pupils, we will consider carefully how best to take pupils' needs into account when deciding how to use their personal information (in line with the requirements of the Data Use and Access Act 2025)

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

It is our responsibility to ensure that the data we share is compliant with the conditions of processing and is shared in a secure manner.

Third parties include:

- HR providers.
- Payroll providers.
- Social Services.
- Recruitment agencies.
- Banks.
- Pension providers – TPS, LGPS, other.
- Local Authorities.
- Department for Education.
- DfE.
- External accountants.
- Occupational health providers.

We abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

We do not send direct marketing material to someone electronically (e.g. via email) unless we have an existing business relationship with them in relation to the services being marketed.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

Sensitive personal data
In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed. An explicit consent form is available at Appendix 1 of this policy for this purpose.

Sensitive data will be shared on a needs basis with appropriate access controls.

Sensitive data will be collected on the following grounds:

- Explicit consent has been given.
- 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 law.
- Processing is necessary for the reasons of substantial public interest, on the basis of Union or Member state law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Data Handling/Sharing (pupil data)
When children leave or join an Omnia Learning Trust school (including in-year transfers), all files (including child protection files) will be transferred in accordance with best practice guidance stipulated in KCSIE.

Safeguarding
The Local Authority will share information with the school when children being admitted to the pupil roll have a social worker and this information will also be requested by the school on the pupil information form. This information will be used to ensure that decisions will be made in the best interest of the child's safety, welfare and educational outcomes.

Privacy by Design and Privacy Impact Assessments
The Trust will act in accordance with the UK GDPR regulations by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities. Data Protection Impact Assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to Omnia Learning Trust's reputation which might otherwise occur.

A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA will be used for more than one project, where necessary. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling.
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences.

The Trust will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes.
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals.
- The measures implemented in order to address risk.

Where a DPIA indicates high risk data processing, the Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

DBS checks and personal data
All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

CCTV
All schools in the Trust use CCTV in various locations to ensure security of the school site. All Trust schools' follow the ICO's guidance for the use of CCTV, and comply with data protection principles. Cameras are not placed in areas where privacy can be breached.

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 for the purposes of safety and security. Data is stored for limited periods of time (as stipulated in the school's CCTV policy).

Any enquiries about the CCTV system should be directed to the DPO.

Academies must register use of their CCTV with the ICO ico.org.uk/registration/new

The Principal, Office Manager, Premises Manager and DPO have access to CCTV images.

Each academy must have a CCTV policy.

Photography
The Trust/academy will always indicate its intentions for taking photographs of pupils and will attain parental permission before publishing them.

If the Trust wishes to use images/video footage of pupils in a publication, such as the Trust website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil. Written consent will be obtained when a pupil starts at one of the Trust's academies. Parents are allowed to withdraw consent for school use of pupil photographs.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Artificial Intelligence
Artificial intelligence (AI) tools are widespread and easy to access. Staff, pupils, and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Omnia Learning Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Omnia Learning Trust will treat this as a data breach, and will follow the personal data breach procedure outlined in this policy.

Data security
We keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Privacy by design and default
Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for ensuring that all data security processes and IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

Storing data securely - Strategic and operational practices
Staff must be clear who the key contact(s) for key school information are (the Information Asset Owners). We have listed the information and information asset owners in the data audit conducted (LGFL Data Asset Registers).

We ensure staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.

All staff are DBS checked and records are held online (SCR Tracker).

We ensure ALL the following school stakeholders sign an Acceptable Use Agreement. We have a system so we know who has signed. Staff must read and refresh knowledge and sign annually.

- staff.
- pupils.
- parents.
- volunteers.

This makes clear all responsibilities and expectations with regard to data security.

- We have implemented approved educational web filtering across all academy networks, ensuring compliance with KCSiE and Prevent guidelines, as well as meeting all statutory requirements set by the DfE.
- We also have an additional layer of monitoring software across our academy networks and ensure all schools meet the filtering and monitoring standards and requirements set out in KCSIE 2025.
- We monitor school e-mails / blogs / online platforms, etc. to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of e-mails / blogs / etc.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
- We require staff to use STRONG passwords for access into our MIS system.
- We require staff to change their passwords into the MIS, USO every 90 days.
- We require that any personal/sensitive material must be encrypted if the material is to be removed from the school, and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff who set up usernames and passwords for e-mail, network access, and other software systems work within the approved system and follow the security processes required by those systems.
- We ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which need no longer be stored.
- In cases when data is stored on printed paper, it is kept in a secure place where unauthorised personnel cannot access it.
- Printed data is shredded when it is no longer needed – use data deletion processes as set out in this policy.
- Secure remote access software is used for accessing school systems from another location.
- Each academy has an Access Control list – defining who has access to data, systems and administrator access is limited to just a few users.
- Network permissions are set correctly so users can only access the data and files they require to carry out their duties.
- All network users have individual logins. There are no shared usernames or passwords.
- Passwords must be adequately complex and changed periodically. These periods will be set for each device – 6 months for Ipads and 3 months for laptops.
- National Cyber Security Centre has useful advice for passwords which the Trust shares with staff.
- We encourage all staff to use a password manager to create and store their passwords.
- Devices such as laptops, tablets and mobile phones must be locked away when not in use.
- Antivirus and malware software are kept up to date as well as operating systems on laptops, tablets and mobile phones.
- Mobile phones are password protected and able to have their content accessed/deleted remotely. Staff will install security measures where available e.g. fingerprint recognition, face recognition, pin numbers etc.

- Staff will inform the Principal/Office Manager/Business Manager immediately if they lose a personal device that has been used to access school systems (including but not limited to Office 365, Outlook, G Suite).
- Screen locks should be in place for users of MIS systems and other software packages containing personal data.
- Emails containing personal data should not be sent from staff/governor/trustee personal accounts.
- Staff should be vigilant of emails with suspicious attachments, from emails addresses who have similar name configurations hyperlinks and proceed cautiously.
- Staff complete basic 'cyber security' training in relation to opening emails, scanning USBs, handling personal data etc.
- Cyber Security Training is held annually at each academy. All staff complete the mandated RPA Scheme Cyber Security training and this is an annual requirement: https://youtu.be/pP2VKWSagE0.
- Wireless network is password protected and encrypted.
- Data stored on CDs or memory sticks is encrypted and locked away securely when not being used. The use of such devices is actively discouraged.
- The DPO must approve any cloud used to store data.
- Servers containing personal data are kept in a secure location or in the cloud, away from general office space.
- Data is regularly backed up in line with the company's backup procedures.
- Data is never saved directly to mobile devices such as laptops, tablets or smartphones.
- Staff must report loss of a school issued device; laptop, mobile phone, Chrome Book, tablet etc. immediately to the Principal/Office Manager/Business Manager.
- Academies must keep a record of third party access to data – e.g. payroll companies, pension providers etc.
- Staff have a secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
- We use the LA's secure system to transfer documents to schools in London, such as references, reports of children.
- We store any sensitive/special category written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We comply with the WEEE directive on equipment disposal, by using an approved disposal company for disposal of IT equipment. For systems, where any protected or restricted data has been held, (such as servers, photocopiers), we get a certificate of secure deletion.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.

Data retention periods

We retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but if relevant, the length of retention will be determined in a manner consistent with published legal and regulatory data retention guidelines.

Documents will be stored in line with guidance stated in the document retention schedule set out by the IRMS (available on the Trust website and Parago).

Data deletion
Disposal of records that have reached the end of the minimum retention period **should be deleted or archived in line with the following guidance in relation to the principle of the UK GDPR that** personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

In each **academy**, **office/business** managers must ensure that records that are no longer required are reviewed as soon as possible under the criteria set out so that only the appropriate records are destroyed.

The local review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained by the organisation for research or litigation purposes.

Whatever decisions are made they need to be documented as part of the Data Retention Policy within the organisation.

Safe destruction of records
All records containing personal information, or sensitive policy information should be made either unreadable or un-reconstructable.

- Paper records should be shredded using a cross-cutting shredder.
- CDs / DVDs / Floppy Disks should be cut into pieces.
- Audio / Video Tapes and Fax Rolls should be dismantled and shredded.
- Hard Disks should be dismantled and sanded.

Any other records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Do not put records in with the regular waste or a skip unless there is no other alternative.

There ***a***re companies who can provide confidential waste bins and other services which can be purchased to ensure that records are disposed of in an appropriate way.

Where an external provider is used it is recommended that all records must be shredded on-site in the presence of an employee. The academy must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction. Staff working for the external provider should have been trained in the handling of confidential documents.

The shredding needs to be planned with specific dates and all records should be identified as to the date of destruction.

It is important to understand that if the records are recorded as to be destroyed but have not yet been destroyed and a request for the records has been received they MUST still be provided.

Where records are destroyed internally, the process must ensure that all records are recorded are authorised to be destroyed by the Principal and the destruction recorded. Records should be shredded as soon as the record has been documented as being destroyed.

Annual data deletion day

Each academy must set aside one day per year to ensure the limits set out in the IRMS Data retention schedule have been followed accurately. Academies may make local decisions about the deletion of pupil data for pupils who have moved schools if they are confident the new schools has safely received and stored the pupils data.

Freedom of Information Act 2000 (FoIA 2000)
The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction.

Office/Business managers should record at least:

- File reference (or other unique identifier);
- File title (or brief description);
- Number of files and date range;
- The name of the authorising Principal; and,
- Date action taken.

Transfer of records to Archives
Where records have been identified as being worthy of permanent preservation arrangements should be made to transfer the records to the County Archives Service. The school should contact the local record office if there is a requirement to permanently archive the records, and the records will continue to be managed via the UK GDPR and the FoIA 2000.

If you would like to retain archive records in a special archive room in the school for use with pupils and parents please contact the local record office for specialist advice.

Transfer of information to other media
Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as microform or digital media. The lifespan of the media and the ability to migrate data where necessary should always be considered.

Consideration should also be given to the legal admissibility of records that have been converted from paper to electronic media. It is essential to have procedures in place so that conversion is done in a standard way. This means that organisations can prove that the electronic version is a genuine original and could not have been tampered with in any way. Reference should be made to 'British Standard 10008:2008 'Evidential weight and legal admissibility of electronic information' when preparing such procedures.

Recording of all archiving, permanent destruction and digitisation of records
Sample appendices are provided for the recording of all records to be used. These records could be kept in an Excel spreadsheet or other database format.

Transferring data internationally
There are restrictions on international transfers of personal data. No data may be transferred outside of the UK without first discussing it with the DPO. Specific consent from the data subject must be

obtained prior to transferring their data outside the UK. Any transfer personal data anywhere outside the UK must be approved by the DPO.

Subject access requests
Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. **No charges** should be made to the data subject. Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within **one month**, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system.

The Trust/Academy has one month to provide a full response to the data subject. Data subjects can be encouraged to submit requests during term time but are under no legal obligation to do so.

If you would like to make a Subject Access Request, you should refer that request immediately to the DPO. We may ask you to help us comply with those requests. There are also restrictions on the information to which you are entitled under applicable law.

Please refer to the Subject Access Request Policy for more information.

Right to be forgotten and to rectification
A data subject may request that any information held on them is rectified, deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where the personal data in question has been disclosed to third parties, the Trust will inform them of the rectification where possible. Where appropriate, the Trust will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex. Where no action is being taken in response to a request for rectification, the Trust will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to restrict processing
Individuals have the right to block or suppress the Trust's processing of personal data. In the event that processing is restricted, the Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future. The Trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Trust has verified the accuracy of the data.
- Where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual.
- Where processing is unlawful and the individual opposes erasure and requests restriction instead.
- Where the Trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If the personal data in question has been disclosed to third parties, the Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so. The Trust will inform individuals when a restriction on processing has been lifted.

The right to data portability
Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller.
- Where the processing is based on the individual's consent or for the performance of a contract.
- When processing is carried out by automated means.

Personal data will be provided in a structured, commonly used and machine-readable form. The Trust will provide the information free of charge. Where feasible, data will be transmitted directly to another organisation at the request of the individual. Omnia Learning Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual. The Trust will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to object
The Trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest.
- Direct marketing.
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling

legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the Trust will offer a method for individuals to object online.

Training
All staff receive training on this policy and related policies and procedures. New joiners will receive training as part of the induction process. Further training on these policies and the law relating to data protection will be provided at least annually or whenever there is a substantial change in the law or our policy and procedure.

Completion of training is compulsory.

All school Governors and Board Directors must also receive training on Data Protection on induction and regularly thereafter.

Data breaches
Staff should notify the Principal or the DPO **immediately** if they are concerned about a possible data breach.

If a breach is discovered outside of term time by a staff member, they should alert the DPO immediately.

Recording data breaches (internal monitoring)
The Trust keeps a record of all reportable and non-reportable data breaches.

All breaches, whether reportable to the ICO or not, must be internally reported to the Principal/Office Manager/DPO and recorded by the DPO on behalf of the Trust.

Reporting breaches to ICO – Reportable Breaches
Data breaches which are considered to be a risk to the rights and freedoms of the individuals involved must be reported to the ICO within 72 hours via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113). If the breach is sufficiently serious to warrant notification to the public, the breach must be reported without undue delay.

If there is a high risk to the rights and freedoms of individuals, data subjects must be notified.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures.

Checklist for data breaches
In the event of a breach which is considered reportable to the ICO, the Trust will follow the ICO's guidance on personal data breaches to include some or all of the following steps as appropriate:

1. Mobilise a crisis management team – Principal, Office/Business Manager, DPO and IT Consultant.
2. Assess level of risk of data breach – no risk/risk/high risk – if unaddressed such as breach is likely to have a significant detrimental effect on individuals /data subjects.
3. Inform the ICO within 72 hours.
4. DPO to keep records of response to the data breach.
5. Identify key internal and external messaging for communications strategy and issue.
6. Secure IT systems.
7. Stop additional data loss.
8. Speak to those affected/involved: If there is a high risk to the rights and freedoms of individuals, data subjects must be notified.
9. Identify key issues and extent of data breach.
10. Review protocols about disseminating information about the breach for everyone involved.
11. Begin an in-depth investigation, using forensics if necessary.
12. Report to police when/if considered appropriate.
13. Notify regulators/consult with legal team/insurers/RPA etc.

What information must a breach notification contain?
1. The nature of the personal data breach including, where possible:
   - the categories and approximate number of individuals concerned; and
   - the categories and approximate number of personal data records concerned.
2. The name and contact details of the data protection officer.
3. A description of the likely consequences of the personal data breach; and
4. A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

Consequences of failing to comply
We take compliance with this policy very seriously. Failure to comply puts both the staff and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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.

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 external IT support provider to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it is appropriate to 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 endeavor to obtain 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
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its local safeguarding partners

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Contact:

If you would like to discuss anything in this policy, please contact:

- Sarah Bellingham, Data Protection Officer, admin@omnialearningtrust.org

Appendix 1

Explicit Consent Form

1. Consent sought:

_____

2. Scope

The consent of the data subject is one of the conditions for the processing of his or her personal data and is within the scope of this procedure. The Omnia Learning Trust and its academy schools need to obtain consent when no other lawful basis applies.

Consent of the data subject is defined by the UK GDPR[1] as '*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'*

Explicit consent is required for the processing of sensitive personal data. Specific conditions apply to the validity of consent given by children in relation to information society services, with requirements to obtain and verify parental consent below certain age limits.

3. Responsibilities

As a data controller, the Omnia Learning Trust and its academy schools, are responsible under the UK GDPR for obtaining consent from the data subject under advisement from the Data Protection Officer.

4. Consent procedure

The Omnia Learning Trust and its academy schools provide clear privacy notices wherever personal data is collected to ensure that consent is informed and that the data subject is informed of their rights in relation to their personal data.

The Omnia Learning Trust and its academy schools demonstrate data subject(s) consent to the processing of his or her personal data or explicit consent for sensitive personal data.

5. Child consent procedure

Where processing relates to a child under 16 years old, the Omnia Learning Trust and its academy schools demonstrates that consent has been provided by the person who is holder of parental responsibility over the child.

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

A. Data Subject details

Title (Mr, Mrs, Miss, etc)	
Surname	
First name	
Current address	
Telephone number	
Email address	
Date of birth	
2 x ID required to confirm name of data subject • Passport • Driving License • Birth certificate • Utility bill (last 3 months) • Vehicle Registration document • Bank statement (last 3 months) • Rent book	

B. Acting on behalf of a Data Subject

Are you acting on behalf of the data subject with their written or other legal authority?	
If yes, please state your relationship with the data subject (parent, legal guardian or solicitor)	
Please enclose proof of written or legal status for acting on behalf of data subject.	
Title	
Surname	
First name	
Current address	
Telephone number	
Email address	

DECLARATION

I, _____ the undersigned and the person identified in (A) above, freely give my consent for the Omnia Learning Trust and its academy schools to use the data stated in section 1 in the manner described.

Signature: Date:

Name of person completing this form:

Or

I, _____ the undersigned and the person identified in (B) above, freely give my consent for the Omnia Learning Trust and its academy schools to use the data stated in section 1 In the manner described on behalf of the person identified in (A) above.

Signature: Date:

Name of person completing this form: