Olive Academies

Data Protection Policy

Document control table	
Title	Data Protection Policy
Date this update approved	August 2025
Approved by	OA MAT board
Date of next review	August 2026 (unless legislation dictates earlier)
Updates	Updated the definitions in section 3 Included a section on cloud computing Updated the information around generative AI technology Included a section on Data Protection Impact Assessments Included a section on Automated decision making and profiling New section on safeguarding
This is an OA central template which must not be modified.	

Contents

Aims

Olive Academies (OA) aims to ensure that all personal data collected about staff, pupils, parents, trustees and AAB members, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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

Legislation and guidance

This policy has due regard to all relevant legislation and statutory guidance 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
- Data Protection Act 2018 (DPA 2018)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- DfE Keeping children safe in education

This policy also has regard to the following guidance:

- 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2012) 'IT asset disposal for organisations'
- DfE (2023) 'Data protection in schools'
- ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record. In addition, this policy complies with our funding agreement and articles of association.

Definitions

Term	Definition
Personal data	For the purpose of this policy, **'personal data'** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.
Sensitive personal data	Sensitive personal data is defined as: • Genetic data • Biometric data • Data concerning health • Data concerning a person's sex life

	• Data concerning a person's sexual orientation Personal data which reveals: • Racial or ethnic origin. • Political opinions. • Religious or philosophical beliefs. • Trade union membership. • Principles. 'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either: • Under the control of official authority or • Authorised by domestic law. The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below: • The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.
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.
Data Protection Officer	A person responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee the trust's data protection processes and advise academies on best practice.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

The data controller

Olive Academies is registered with the ICO and will renew this registration annually or as otherwise legally required. The OA board of trustees is the Data Controller.

Our academy/school processes personal data relating to parents, pupils, staff, trustees and academy/school advisory board (AAB) members, visitors and others, and therefore are data processors.

Roles and responsibilities

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

Board of trustees

The board of trustees, as the Data Controller, has overall responsibility for ensuring that the trust and our academy/school complies with all relevant data protection obligations.

Data protection officer

The data protection officer (DPO) is responsible for:

- Overseeing the implementation of this policy.
- Monitoring compliance with data protection law and developing related policies and guidelines where applicable.
- Providing annual training for all staff on the risks, limitations, and lawful processing requirements when using generative artificial intelligence (AI) technologies.

The DPO will provide an annual report of their activities directly to the MAT board and, where relevant, report to the board their advice and recommendations on academy/school data protection issues.
The DPO is also the first point of contact for individuals whose data the academy/school processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Kuda Mika and is contactable via kuda.mika@oliveacademies.org.uk

Head of Academy/School

The head of academy/school acts as the representative of the data controller on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the academy/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 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

Data protection principles

The UK GDPR is based on data protection principles that our academy/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 academy/school aims to comply with these principles.

Collecting personal data

Lawfulness, fairness and transparency
OA 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 academy/school can **fulfil a contract** with the individual, or the individual has asked the academy/school to take specific steps before entering into a contract
- The data needs to be processed so that the academy/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 academy/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 academy/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, OA will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health** reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, OA will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

OA will always consider the fairness of our data processing and ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

If OA offer online services to pupils, such as classroom apps, and intends to rely on consent as a basis for processing, parental consent, where the pupil is under 13, will be sought (except for online counselling and preventive services).

Limitation, minimisation and accuracy
OA will only collect personal data for specified explicit and legitimate reasons and will explain these reasons to the individuals when first collecting their data.

If OA want to use personal data for reasons other than those given when we first obtained it, the individuals concerned will be informed consent sought where necessary.

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the trust's data retention policy.

Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- OA needs to liaise with other agencies – OA will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, OA 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 OA 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

OA will also share personal data with law enforcement and government bodies where legally required to do so.

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

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

Subject access requests and other rights of individuals

Subject access requests
Individuals have a right to make a 'subject access request' to gain access to personal information that the academy/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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguarding provided of the data is being transferred internationally

Subject access requests can be submitted in any form, but OA may be able to respond to requests more quickly if they are made in writing and 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.

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

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

Children aged 12 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 academy/school 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.

Responding to subject access requests
When responding to requests, OA:

- may ask the individual to provide two forms of identification
- may contact the individual via phone to confirm the request was made
- will respond without delay and within 30 days of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- 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. OA will inform the individual of this within 1 month, and explain why the extension is necessary

OA may 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 being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- would include another person's personal data that cannot reasonably be anonymised, and OA do not have the other person's consent, and it would be unreasonable to proceed without it
- is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, OA may refuse to act on it or charge a reasonable fee which takes into account administrative costs. OA will consider whether the request is repetitive when making this decision.

When OA refuse a request, the individual will be informed of the reason and that they have the right to complain to the ICO or that they can enforce their subject access request right through the courts.

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 OA are collecting their data about how OA use and process it (see section 7), individuals also have the right to:

- withdraw their consent to processing at any time
- ask OA to rectify, erase or restrict processing of their personal data (in certain circumstances)
- prevent use of their personal data for direct marketing
- object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- be notified of a data breach in certain circumstances
- make a complaint to the ICO
- ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

Parental requests to see the educational record

There is no automatic parental right of access to the educational record of their child within an academy/ school, but OA follows the guidance to all maintained schools which is that parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request. The academy/school may charge a fee to cover the cost of supplying an educational record and only applies as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

CCTV

OA academies/schools use CCTV in various locations around the academy/school site to ensure it remains safe. OA will adhere to the ICO's guidance for the use of CCTV and will also follow the trust's CCTV systems policy which is available on request.

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

Any enquiries about the CCTV system should be directed to the head of academy/school.

Photographs and videos

As part of our academy/school activities, photographs and recorded images of individuals may be taken. The academy/school will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials and clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at academy/school events for their own personal use are not covered by data protection legislation. However, OA 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.

Academies/schools will obtain written consent from parents/carers, or from pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials. Where parental consent is required, it will be clearly explained how the photograph and/or video will be used to both the parent/carer and pupil. Where parental consent is not required, it will be clearly explained to the pupil how the photograph and/or video will be used.

Where OA take photographs and videos, uses may include:

- Within academy/school on notice boards and in academy/school magazines, brochures, newsletters, etc.
- Outside of academy/school by external agencies such as the academy/school photographer, newspapers, campaigns
- Online on our academy/school website or social media pages

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

When using photographs and videos in this way OA will not accompany them with any other personal information about the child, to ensure they cannot be identified. OA provide staff with guidelines on the use of images within the ICT and online safety policy.

Cloud computing

For the purposes of this policy, **'cloud computing'** refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the school accessing a shared pool of ICT services remotely via a private network or the internet.

All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

If the cloud service offers an authentication process, each user will have their own account. When assessing any cloud-based or AI-powered service, the academy/school will ensure that the provider demonstrates UK GDPR compliance, provides explicit guarantees regarding non-retention of input data, and allows the academy/school to audit or verify compliance where necessary. The use of any cloud services which involve AI processing will be subject to a prior risk assessment and will require a DPIA where personal data is involved. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the academy/school.

All files and personal data will be encrypted before they leave a academy/school device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DPO immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

As with files on academy/school devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the school should unauthorised access, deletion or modification occur and ensure ongoing compliance with the academy/school's policies for the use of cloud computing.

The academy/school's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

The DPO will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the trust's Data Protection Policy.
- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the school decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the school is prepared to accept that risk.
- Monitor the use of the academy/school's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the headteacher

Artificial intelligence (AI)

The academy/school recognises that generative AI technologies involve the processing of extensive datasets and may pose increased risks to data privacy and security.

Staff and pupils must not input personal, identifiable, or sensitive data into generative AI platforms unless the system has been formally assessed, and explicit approval has been granted following a full DPIA.

Only AI systems that meet UK GDPR standards and have been assessed for data minimisation, security, transparency, and retention practices will be used in school operations.

Use of generative AI tools must comply with the school's Acceptable Use Policy. Individuals must not rely solely on AI-generated outputs without appropriate human oversight and validation.

Any incidents, breaches, or concerns arising from the use of AI tools must be reported immediately to the DPO and will be investigated in line with the school's data breach procedures.

Automated decision making and profiling

The academy/school will only ever conduct solely automated decision making with legal or similarly significant effects if the decision is:

- Necessary for entering into or performance of a contract.
- Authorised by law.
- Based on the individual's explicit consent.

Automated decisions will not concern a child nor use special category personal data, unless:

- The academy/school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest.

The Head of Academy/School will conduct a Data Protection Impact Assessment (DPIA) for automated decision making to mitigate risk of errors, bias and discrimination.

The school will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.

Generative AI systems will not be used to make solely automated decisions with significant effects on individuals, such as decisions regarding academic grading, behaviour sanctions, admissions, or staff appraisals, unless a suitably qualified person reviews and authorises the decision-making outcome.

Individuals have the right not to be subject to a decision when both of the following conditions are met:

- It is based on automated processing, e.g. profiling
- It produces a legal effect or a similarly significant effect on the individual

The academy/school will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the academy/school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Data protection by design and default

OA will put measures in place to show that integrated data protection is in place in all 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 academy/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; also keeping a record of attendance at training
- Regularly conducting reviews and audits to test our privacy measures and make sure the whole trust is compliant
- Appropriate safeguards being put in place if personal data is transferred outside of the UK, where different data protection laws will apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of OA academies/schools and DPO and all information OA are required to share about the use and process of personal data (via OA privacy notices)
    - For all personal data held, maintaining an internal record of the type of data, data subject, how and why OA are using the data, any third-party recipients, how and why the data is stored, retention periods and how OA are keeping the data secure

Data Protection Impact Assessments (DPIAs)

DPIAs will be used in certain circumstances to identify the most effective method of complying with the academy/school's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will be conducted prior to the implementation of any generative AI tools where the processing of personal data is involved, particularly if the AI tool automates decision-making, involves profiling, or carries a risk of bias, inaccuracy, or data misuse.

A DPIA will include specific evaluation of the risks associated with AI systems, including fairness, accuracy, accountability, transparency, and security, in accordance with the DfE's 'Generative artificial intelligence in education (2025)' guidance.

DPIAs will allow the academy/school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the trust/academy/school's reputation which might otherwise occur. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, and 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 use of CCTV

The academy/school 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 school will consult the ICO to seek its opinion as to whether the processing operation is compliant

Data security and storage of records

OA 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 academy/school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access academy/school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or trustees who store personal information on their personal devices are expected to follow the same security procedures as for academy/school-owned equipment (see our ICT acceptable user agreement on acceptable use)
- Where OA need to share personal data with a third party, due diligence will be carried out and reasonable steps will be taken to ensure it is stored securely and adequately protected (see section 8)

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 OA cannot or do not need to rectify or update it.

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

Personal data breaches

OA will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, staff will follow the procedure set out in Appendix 1.

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

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

Safeguarding

Olive Academies understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

The **academy/school will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect pupils. The governing board will ensure that staff are:**

- Confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'.
- Aware that information can be shared without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a pupil in a timely manner.

The **academy/school** will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

The **academy/school** will aim to gain consent to share information where appropriate; however, staff will not endeavour to gain consent if to do so would place a child at risk. The **academy/school** will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

Pupils' personal data will not be provided where the serious harm test is met. Where there is doubt, the academy/school will seek independent legal advice.

Training

All staff and trustees and AAB members are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the academy/school's processes make it necessary.

Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed **annually** unless legislation requires otherwise and approved by the Board of Trustees.

Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- CCTV systems policy
- ICT and online safety policies
- GDPR privacy notices for staff, trustees, pupils, and candidates
- Child protection and safeguarding policy
- Record retention policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

Identifying and actions for potential breaches
On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.

The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- lost
- stolen
- destroyed
- altered
- disclosed or made available where it should not have been
- made available to unauthorised people

The DPO will alert the head of academy/school and the CEO or DCEO.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen and 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

The DPO will document the decision (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored with DPO at the central team's office.

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

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 of action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches/ potential breaches will be stored with DPO at the central team's office.

The DPO and head of academy/school will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

OA will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information and 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 ICT department to recall it.
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, OA will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Other types of breach that you might want to consider could include:

- details of pupil premium interventions for named children being published on the academy/school website
- non-anonymised pupil exam results or staff pay information being shared with AAB

- an academy/school laptop containing non-encrypted sensitive personal data being stolen or hacked
- the academy/school's cashless payment provider being hacked and parents' financial details stolen