CARLTON
ACADEMY TRUST

Carlton Academy Trust
General Data Protection Regulation (GDPR) / Data Protection Policy

Approved on behalf of Trustees:	**Roger Butterfield**
Review Date:	**July 2023**
Next Review:	**July 2024**

Glossary

DPO:	Data Protection Officer
GDPR:	General Data Protection Regulation
HOS:	Head of School
ICO:	Information Commissioners Office
Parents:	Umbrella term also including carers
SAR:	Subject Access Request

Section One: Policy Aims, Responsibilities and Definitions

Aims

This policy aims to ensure that all personal data collected by the trust is stored and processed in accordance with UK Data Protection Law. It applies to all staff and any organisations or personnel commissioned by the trust. It meets the requirements of the UK GDPR and is based on guidance published by the ICO.

The Trust and its schools are classed as 'Data Controllers' as they process personal data of parents, students, staff, trustees, members, or governors, being registered with the ICO for this purpose.

Responsibilities

Trustees

Have ultimate responsibility for ensuring schools and central trust team comply with the provisions of this policy.

DPO

The Director of Data is the Trust DPO with operational responsibility for implementation of this policy, data compliance, development of effective data protection procedures, and acting as the first point of contact with the ICO.

HOS

Are responsible for the effective management of data within their schools.

All staff

Have the following responsibilities in relation to data:

- Collect, store and process personal data in accordance with this policy.
- Immediately report any suspected data breach to the DPO, so that the trust can remain within the 72-hour ICO reporting guidelines.
- Inform the DPO if they have any questions or concerns about the storage, protection, or use of personal data, or where others may not be following trust data protection procedures.

Principles of Data Protection

- Data is processed lawfully, fairly, and transparently in ways that individuals would reasonably expect.
- Data is collected for specified, explicit and legitimate purposes.
- Data collected is adequate, relevant, and limited to what is necessary to fulfil the processing purpose.
- Data collected is accurate and kept up to date.
- Data is kept for no longer than is necessary for the purposes for which it is processed.
- Data is processed in a secure way.

Definitions

Personal Data: Any information relating to an identified or identifiable living person including their physical, physiological, genetic, mental, economic, cultural, or social identity.

Special Category Personal Data: Personal data which is more sensitive and needs greater protection. These include:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetics
- Biometrics when used for identification purposes.
- Physical or mental health.
- Sex or sexual orientation

Data Processing: Any task relating to personal data such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing may be automated or manual.

Data Subject: The person whose data is being processed.

Data Controller: Person or organisation that defines the purposes and means of processing of personal data.

Data Processor: Person or other body other who process personal data on behalf of the data controller.

Personal Data Breach: Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data.

Section Two: Processing Data and Subject Access Requests

The Trust only processes personal data when an individual has freely given their consent, for the following purposes:

- Fulfilment/due diligence of a contract.
- Compliance with a legal duty.
- Ensuring the vital interests of the individual.
- Enabling the school or trust as a public authority to perform a task in the public interest.
- Protecting the interests of the trust or third party providing that the individual's rights and freedoms are not compromised.

Special Category Data

Must only be processed under one or more of the following conditions:

- Appropriate consent has been received.
- The data must be processed to exercise obligations or rights in relation to employment, social security, or statutory requirements.
- To protect the vital interests of the individual or other person, where the individual is physically or legally incapable of giving consent.
- The data has already been made manifestly public by the individual.
- For the establishment, exercise, or defence of legal claims.
- For reasons of substantial public interest as defined by legislation.
- For health or social care purposes and is completed by or under the direction of a health or social work or other authorised professional.
- For archiving, scientific, historical, or statistical purposes in the public interest.

Criminal Record Data

Criminal record data may be processed:

- With appropriate consent.
- To ensure the vital interests of the individual or another person, where they are physically or legally incapable of giving consent.
- If the data has already been made public.
- If the data needs to be processed in connection with legal proceedings; to obtain legal advice; or establishment, exercise, or defence of legal rights.
- For reasons of substantial public interest as defined by legislation.

Limitation, Minimisation and Accuracy

The trust collects personal data for specified, explicit, and legitimate reasons, necessary for completion of its duties. Reasons will be explained when it is collected. Should we subsequently intend using data for other reasons, we will inform the individual/s concerned to obtain their consent. We strive to keep data accurate with inaccurate data rectified or erased. When data is no longer needed, data will be deleted or anonymised in accordance with the Information and Records Management Society's toolkit for schools.

Sharing Personal Data

We do not share personal data without consent except in specific circumstances:

- When individuals are at risk.
- To enable effective liaison with police, local authority social care, or other government agencies to reduce crime or fraud, assist legal proceedings, help in the collection of taxes, satisfy safeguarding requirements, or assist research or statistical analysis.
- To assist emergency services responding to an emergency.
- When suppliers or contractors need data to enable them to provide services. In doing this we will:

    a. Only appoint companies who can provide sufficient guarantees that they comply with UK data protection law.
    b. Create a data sharing agreement to ensure the fair and lawful processing of any personal data.
    c. Only share data necessary for them to carry out their service or keep them safe while working with us.

Where we transfer personal data internationally, we do so in accordance with UK data protection law.

SARs

Data subjects may make SARs to access personal information that the trust holds about them.

The DPO should immediately be informed when any request is made. SARs can be submitted in any form but preferably in writing as they are easier to record and process.

SARs for children below the age of 13 must be made by parents, as they are considered not mature enough to make an informed decision.

SARs must include the following details:

- Name, address, and contact details (phone, email).
- Details of the information requested.

Requests are commonly made to:

- Confirm that personal data is being processed, type of data, and for what purpose.
- Identify who data has been/will be shared with.
- Request a copy of the data.
- Determine how long the data will be stored for, or the criteria used to determine this.
- Request clarification, erasure, restriction, or objection to processing.
- Confirm what safeguards are applied where data is transferred internationally.
- Identify the source of data being processed, when not provided by the individual.

Responding to SARs:

The trust will need to ensure any request is genuine. It does this by requesting two forms of identification and contacting the individual by phone to confirm the request has been made from them.

Requests must be responded to without delay and always within one month of confirmation of identity. This may exceptionally extend to three months where requests are complex or numerous, with the individual being informed of this within one month and why any extension is necessary.

We will not disclose information where it:

- May cause serious harm to the physical or mental health of the individual.
- Would put a child at risk of abuse, or contrary to their best interests.
- Would include another person's personal data that can't reasonably be anonymised, don't have the other person's consent and would be unreasonable to proceed without it.
- Is part of sensitive documents such as those relating to crime, immigration, legal proceedings, legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

Where a request is deemed unreasonable or excessive, the trust may refuse to act or charge a fee proportionate to administrative costs. A request may be deemed unfounded or excessive if it is repetitive or asks for further copies of the same information. Where a request is refused, we will inform the individual of the reasons without delay and that they have the right to complain to the ICO or enforce their rights through the courts.

Section Three: Miscellaneous

Artificial intelligence (AI)

AI tools are now widespread and easy to access. Staff, pupils and parents may be familiar with generative chatbots such as ChatGPT and Google Bard. Carlton Academy 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, we will treat this as a data breach, and will follow the personal data breach procedures.

Biometric Systems

Consent must be obtained from all parties who use biometric data systems. This may be withdrawn at any time, after which the trust must ensure that any data is deleted, and these individuals can use alternative systems to access the relevant services. Where a student refuses the use of their biometric data, the trust must not do so irrespective of parental consent.

CCTV

Trust CCTV use adheres to ICO guidance. It does not require consent for its use but must be clearly signposted where it is in use.

Data Breaches

When a potential breach is discovered, this must immediately be reported to the DPO. They will investigate and determine whether a breach has occurred. Where occurring, the DPO will determine whether this should be reported to the ICO. They will consider whether it is likely to negatively affect people's rights and freedoms, cause them any physical, material, or non-material damage, or emotional distress through:

- Discrimination.
- Identity theft or fraud.
- Financial loss.
- Unauthorised reversal of pseudonymisation such as key coding.
- Damage to reputation.
- Loss of confidentiality.
- Any other significant economic or social disadvantage to the individual(s) concerned.

Where a report is required, it must be made to the ICO within 72 hours in accordance with their reporting guidelines. Where full details of the breach are not available within this 72-hour period, this must be explained to the ICO and forwarded without delay once obtained.

Where there is a high-risk data breach, the DPO will promptly inform all individuals in writing of their name and contact details, likely consequences of the breach, and measures that have been or will be taken to deal with it.

The DPO will coordinate reasonable efforts to contain and minimise the impact of any breach, and where relevant meet with the HOS and CEO to consider measures to prevent recurrence. They will also notify any relevant third parties such as police, insurers, banks, or credit card providers.

Recording Data Breaches

The DPO records all breaches, irrespective of whether they are reported to the ICO. Records include the circumstances, consequences, and actions taken to contain it and prevent recurrence.
The trust will act to mitigate the impact of data breaches, especially those involving sensitive information. The effectiveness of these actions will be reviewed and used to inform future procedures.

Where special category data is accidentally shared through email to unauthorised people, the sender must attempt to recall the email without delay. If the sender is unavailable or cannot recall the message, IT personnel will recall it. Where a recall is unsuccessful, the DPO will contact the people who received the email in error, requesting that they delete the information and do not share, publish, save, or replicate it in any way. The DPO must then obtain written confirmation that they have complied with the request. The DPO may carry out an internet search to check that information has not been made public, requesting the removal and deletion of data where this has occurred.

Staff receiving special category personal data in error must alert the sender and DPO without delay.

Data Protection by Design and Default

The Trust ensures high data protection standards through:

- Appointing a suitably qualified and resourced DPO.
- Only processing personal data that is necessary for the stated purpose and adhering to data protection principles and law.
- Completing data protection impact assessments where processing of personal data presents a high risk.
- Increasing staff awareness of data protection regulations, policy, and practice.
- Completing regular data protection reviews and audits.
- Applying appropriate safeguards when data is transferred outside of the UK, where different data standards are applied.
- Maintaining accurate records of processing activities. This includes what data is collected, purpose, how it will be processed, third party processors, transfers outside the UK and safeguards, retention periods, and how we keep data secure.

Data Protection Rights

Data subjects have the right to:

- Withdraw their consent to processing at any time.
- In specific circumstances, request rectification, erasure, or restriction of processing.
- Deny use of their personal data for marketing purposes.
- Object to processing based on public interest, official authority, or legitimate interests.
- Challenge decisions based solely on automated decision-making or profiling.
- Be notified of a data breach (in certain circumstances).
- Make a complaint to the trust or ICO.
- Ask for their personal data to be transferred to a third party in a structured, established and machine-readable format (in certain circumstances).

Data Security and Storage

The Trust takes measures to safeguard personal data and keeps it safe from unauthorised or unlawful access, alteration, processing, or disclosure, accidental or unlawful loss, destruction, or damage.

Specific measures include:

- Paper records and laptops/electronic devices containing personal data securely locked or stored when not in use.
- Papers containing confidential personal data not being left on desks or other places where there is general access or can easily be accessed by other people.
- Use of secure passwords to access school computers, laptops, and other electronic devices, which are changed at regular intervals.
- Use of encryption software to protect portable devices and removable media such as laptops and USB devices. E-Mails containing any personal or sensitive data must be sent password protected or via end-to-end secure encryption such as Galaxy Key.
- Staff, students, trustees, members, or governors who store personal information on their personal devices following the same security procedures as for trust devices.
- Taking reasonable steps to ensure data is stored securely and adequately protected when shared with a third-party processor.

Disposal of Data Records

The trust securely disposes of personal data that is no longer needed. Paper-based records are shredded, while electronic records are overwritten or deleted. Third party providers must provide guarantees that they comply with data protection law for this purpose as codified in the guidance provided by the Information and Records Management Society.

Photographs and Videos

Schools must obtain written consent from parents of students up to the age of 13 for the use of photographs and videos for communication, marketing, or promotional purposes. Consent must also explain for what purposes data will be used. Consent can be provided by students aged 13 years and over.

Consent can be refused or withdrawn at any time. If consent is withdrawn, the content must be destroyed or deleted and not distributed any further. Schools must not accompany photographs or videos with any information that could identify the child.

Photographs or videos taken by parents at school events for personal use are not covered by data protection legislation. However, it is good practice for schools to request that for safeguarding reasons photographs or videos of other pupils are not shared through any means unless other parents have provided consent.

Requests to View Educational Records

There is no automatic parental right of access to their child's educational records and will be decided on a case-by-case basis. Requests must be submitted in writing to the DPO and include their full name, address, and details of the information they request.

Any staff member receiving a request to see educational records should immediately inform the DPO.

Training

All Staff are provided with annual data protection training and data protection will form part of CPD where changes to legislation, guidance or the Trust policies make it necessary. This also includes the requirement to alert without delay the sender and DPO when they receive special category data in error.