



**CARLTON**  
ACADEMY TRUST

## **General Data Protection Regulation (GDPR) / Data Protection Policy**

**Approved on behalf of Trustees:**

**Roger Butterfield**

**Review Date:**

**June 2025**

**Next Review:**

**June 2026**



## **Glossary**

<b>ACOO</b>	Assistant Chief Operating Officer
<b>COO:</b>	Chief Operating Officer
<b>DPO:</b>	Data Protection Officer
<b>GDPR:</b>	General Data Protection Regulation
<b>HOS:</b>	Head of School
<b>ICO:</b>	Information Commissioners Office
<b>IRMS:</b>	Information and Records Management Society
<b>Parents:</b>	Umbrella term also including carers and legal guardians
<b>SAR:</b>	Subject Access Request



## **Section One: Policy Aims, Responsibilities and Definitions**

### **Aims and Scope**

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, personnel or organisations commissioned by the trust or its schools. It meets the requirements of UK GDPR and based on ICO guidance. The trust and its schools are 'Data Controllers' as they process personal data and are registered with the ICO for this purpose.

This policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005 for Special Educational Needs Schools, which gives parents the right of access to their child's education record, trust funding agreement and articles of association.

### **Definitions**

**Data Controller:** Person/organisation defining the purpose and methodologies for processing personal data.

**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 Processor:** Person or organisation that process data on behalf of the data controller.

**Data Subject:** The person whose data is being processed.

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

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

**Special Category Personal Data:** Sensitive personal data which needs greater protection:

- Racial or ethnic origin.
- Political affiliations or beliefs.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic or biometric information.
- Physical or mental health.
- Sex and sexual orientation.

### **Principles of Data Protection**

Data is:

- Processed, lawfully, fairly, and transparently in ways that individuals would reasonably expect.
- Collected for specified, explicit and legitimate purposes.
- Collection is adequate, relevant, and limited to what is necessary to fulfil the processing purpose.
- Accurate and where necessary kept up to date.
- Kept for no longer than is necessary for its processing purpose.
- Processed in a way that ensures it is appropriately secure.



## Responsibilities

**Trustees:** Ensuring all staff comply with the provisions of this policy.

**DPO:** The COO 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. The trust DPO is Darren Harvey-Hill and can be contacted on DHH@catrust.uk.

**HOS:** Responsible for the effective management of data within their schools.

### **All staff**

- Collect, store and process personal data in accordance with policy guidelines.
- 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 where they have concerns about the storage, protection, or use of personal data, or where others may not be following trust data protection procedures.



## **Section Two: Processing Data and Subject Access Requests**

The trust processes personal data for six lawful reasons:

- 1) Compliance with legal obligation.
- 2) Fulfilment of contract or contract due diligence.
- 3) Ensuring the vital interests of the individual.
- 4) Public interest.
- 5) Legitimate interests.
- 6) The individual (or parent when appropriate) has freely given clear consent.

### **Special Category Data**

Must only be processed with correct consents:

- To exercise obligations or rights in relation to employment, benefits, 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 when completed by or under the direction of a health, social work or other authorised professional.
- For archiving, scientific, historical, or statistical purposes in the public interest.
- To ensure the vital interests of the individual.

### **Criminal Record Data**

May be processed with appropriate consent:

- To ensure the vital interests of the individual or other 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; obtain legal advice; or establishment, exercise, or defence of legal rights.
- For reasons of substantial public interest.

### **Limitation, Minimisation and Accuracy**

The trust collects personal data for specific, legitimate reasons which are explained during collection. Should data subsequently be used for other reasons, we will inform the individual/s concerned to obtain their consent. We strive to keep data accurate, with inaccurate data corrected or erased. When data is no longer needed, data will be deleted or anonymised in accordance with the IRMS toolkit for schools.

### **Sharing Personal Data**

Data will only be shared without consent in specific circumstances:

- When individuals are at risk.
- To assist police, local authority social care, or other government agencies to reduce crime, 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.
- Enabling suppliers or contractors to provide services. The trust will only appoint companies who can provide sufficient guarantees they comply with UK data protection law. A data sharing agreement will be



made to ensure fair and lawful processing of personal data, and ensure they only share data necessary to carry out their service or safeguard staff interests.

## **SAR's**

The DPO should immediately be informed when a request is made. Requests must include the individuals' name, address, and contact details (phone, email) and full details of information requested.

Requests can be for:

- Confirmation that personal data is being processed, type, purpose and with whom it is being shared.
- Request a copy of data held.
- Determine how long data will be stored, or criteria to determine this.
- Request clarification, erasure, restriction, or objection to processing.
- Identify the source of data being processed, where not provided by the individual.

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.

Requests must include the following details:

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

SARs from third parties (social workers, police, health care providers, other educational establishments/settings) must be accompanied by the authorising request (court orders, police requests for disclosure of information) or email formally requesting information.

## **Responding to SARs**

The trust will ensure requests are genuine by requesting two forms of identification and independently contacting the requestor by phone to confirm the request has been made by them.

Requests must be acted upon without undue delay, and always within one month of confirmation of identity. This may be extended 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, consent has not been obtained 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. When a request is refused, the individual will be informed of the reasons without delay and that they have the right to complain to the ICO or legally enforce their rights.



## **Section Three: Miscellaneous**

### **Artificial intelligence (AI)**

To ensure personal and sensitive data remains secure, this type of data must not be entered into generative AI tools. Where occurring, this will be treated as a data breach. The Trust Artificial Intelligence Policy, must be read in conjunction with this policy.

### **Biometric Systems**

Consent must be obtained when biometric data is processed. Consent may be withdrawn at any time, after which data must be deleted.

### **CCTV**

CCTV usage adheres to ICO guidance. It does not require consent, but its' use must be clearly signposted. Only authorised and nominated staff are to have access to CCTV and the sharing of images / CCTV footage is to be cleared with the Trust DPO, prior to sharing, this is especially important in relation to parents and any third parties.

### **Data Breaches**

When a breach or potential breach is discovered, this must be immediately reported to the DPO who will determine whether this should be reported to the ICO. They will consider whether the breach is likely to negatively affect rights and freedoms; cause physical, material, 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.

Reports must be made within 72 hours. Where full details are not available within this time frame, this must be explained to the ICO and details forwarded without delay once available.

When there is a high-risk data breach, the DPO will promptly inform all affected individuals in writing, providing name and contact details, outlining likely consequences of the breach, and measures that have been or will be taken to manage and minimise its' impact. They will also notify any relevant third parties such as police, insurers, banks, or credit card providers.

The DPO logs all breaches, detailing the circumstances, consequences, and actions taken to contain and prevent recurrence. The effectiveness of these actions will be reviewed and used to inform future practice.

Where special category data is shared through email in error, the sender must attempt to recall the message without delay. If the sender is unavailable or cannot recall the message, IT personnel should be contacted to do this.

Where unsuccessful, the DPO will contact the receiving person/s requesting that they delete the information and do not share, publish, save, or replicate it in any way, obtaining written confirmation they have complied with this request. The DPO may carry out an internet search to check that information has not been made public, requesting its' removal and deletion where found.



It is the responsibility of all staff receiving special category personal data in error to alert the sender and DPO without delay.

### **Data Protection by Design and Default**

The trust ensures high standards of data protection 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 data protection reviews and audits.
- Applying appropriate safeguards when data is transferred outside of the UK, where different data standards may apply.
- Maintaining accurate records of processing activities.

### **Data Protection Rights**

Data subjects have the right to:

- Withdraw their consent to processing at any time.
- Request rectification, erasure, or restriction of processing (specific circumstances).
- 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 (specific circumstances).
- Ask for their personal data to be transferred to a third party in a structured, established, and machine-readable format (specific circumstances).

### **Data Security and Storage**

The trust takes measures to safeguard personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, accidental or unlawful loss, destruction, or damage. Examples include:

- Paper records, laptops, personal computers, electronic devices containing personal data securely locked or stored when not in use.
- Papers containing confidential personal data not left on desks or places where there is general access or easily accessed by other people.
- Use of secure passwords to access school computers, laptops, or other electronic devices which are changed at regular intervals.
- Use of encryption software for portable devices and removable media such as laptops.
- E-Mails containing any personal or sensitive data must be password protected or sent via secure end-to-end secure encryption.
- Ensuring 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 when no longer needed. Paper records are shredded with electronic records overwritten or deleted. Third party providers must guarantee that they comply with data protection law as codified in IRMS guidance.

### **Photographs and Videos**



Schools must obtain written parental consent of students up to the age of 13 for the use of photographs and videos for communication, marketing, or promotional purposes. Consent must explain what purposes data will be used. Consent must be obtained from students aged 13 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 further. Schools must not accompany photographs or videos with any information which could indicate the identity of a 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 unless relevant parents or students have provided their consent.

### **Requests to View Educational Records**

Any request to see educational records should immediately be referred to the DPO.

There is no automatic parental right to access their child's educational records, with access decided on individual merit. Requests must be submitted in writing to the DPO listing full name, address, and details of the information they request.

Parents of children under the age of 18 attending a trust special needs school have the right to access their child's educational record within 15 term days of receipt of a written request.

### **Training**

All staff undertake annual data protection training.

