CARLTON
ACADEMY TRUST

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

Signed on behalf of the trustees:	**R Butterfield**
Reviewed:	**September 2021**
Next Review:	**September 2022**

Aims and Policy Scope

This policy aims to ensure that all personal data collected by the Trust (staff, students, parents/carers, governors, visitors) is stored and processed in accordance with UK Data Protection Law. This policy applies to all personal data irrespective of format. It applies to all staff and any organisations or personnel commissioned by the Trust.

Legislation and Guidance

This policy meets the requirements of the 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 and the Data Protection Act 2018 (DPA 2018). It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR. It meets the requirements of the Protection of Freedoms Act 2012 when referring to any use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with our funding agreement and articles of association.

Responsibilities

Trustees

Carlton Trustees have ultimate responsibility for ensuring all schools comply with the provisions of this policy.

Data Protection Officer (DPO)

The Trust Director of Facilities and Compliance is the Trust Data Protection Officer (DPO). They have operational responsibility for implementation of this policy, monitoring compliance and developing effective data protection procedures. They will provide an annual data protection report to Trustees. The DPO also acts as first point of contact for the Information Commissioners Office (ICO).

Heads of School

Heads of School are responsible for the effective management of data in line with this policy and procedures as defined by the DPO.

All staff

Staff must collect store and process personal data in accordance with this policy. They must also ensure they:

- Immediately report any suspected data breach to the DPO, so that the Trust can stay within the ICO 72-hour reporting guidelines.
- Refer to the DPO if they have any questions or concerns about the storage, protection or use of personal data, or have concerns that others aren't following Trust policy or procedures.

Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable living individual. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. This includes: ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username
Special Categories of Personal Data	Personal data which is more sensitive and so needs greater protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes ● Health – physical or mental ● Sex life or sexual orientation
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 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.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Data Protection Principles

All Trust schools adhere to the following UK GDPR/data protection principles:

- Data is processed lawfully, fairly and in a transparent manner
- It is collected for specified, explicit and legitimate purposes
- It is 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

The Trust will always consider the fairness of our data processing, ensuring that we don't handle personal data in ways that individuals would not reasonably expect or have unjustified adverse effects.

Collecting Personal Data

The Trust will only process personal data under one of 6 lawful bases, as follows:

- Fulfilment of a contract, or an individual has asked the school/Trust to take specific steps before entering into a contract
- Compliance with a legal obligation
- Ensure the vital interests of the individual e.g. to protect someone's life
- Enable the Trust, as a public authority, to perform a task in the public interest
- Protect the legitimate interests of the Trust or third party, provided that the individual's rights and freedoms are not overridden.
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent.

Special Category Data

Special categories of personal data will only be processed where one of the following statutory conditions are met:

- The individual (or their parent/carer when appropriate in the case of a student) 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 by 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.

Criminal Offence Data

The processing of criminal offence data will meet both a lawful basis and a condition set out under data protection law, as follows:

- The individual (or their parent/carer when appropriate in the case of a student) 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.

Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit, and legitimate reasons, which will be explained to individuals when we first collect their data.

If we want to use personal data for reasons other than those given when first obtained, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in completion of their duties. We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased, as appropriate.

In addition, 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 Information and Records Management Society's toolkit for schools.

Sharing Personal Data

We will not normally share personal data without consent from the individual, but there are certain circumstances where we may be required to do so. These commonly include:

- Circumstances relating to a student or parent/carer that places the safety of staff at risk.
- Ensure effective liaison with police, local authority social care or other government agencies in order to reduce crime; tackle fraud; assist legal proceedings; help in the collection of taxes; satisfy safeguarding requirements; assist research or statistical analysis
- Emergency services or local authorities to help them respond to an emergency situation
- When Trust suppliers or contractors need data to enable them to provide services to our staff and students. When doing this, we will:
    - Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with UK data protection law.
    - Establish a data sharing agreement with the supplier or contractor to ensure the fair and lawful processing of any personal data we share.
    - Only share data necessary for the supplier/contractor needs to carry out their service or keep them safe while working with us.

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

Subject Access Requests

Individuals have a right to make a 'Subject Access Request' to gain access to personal information that the Trust holds about them. The DPO should be immediately informed of any requests.

Requests commonly comprise:

- 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.
- Where relevant, the existence of the right to request clarification, erasure or restriction, or to object to such processing.
- The right to lodge a complaint with the ICO or other supervisory authority.
- The safeguards provided if the data is being transferred internationally.
- The source of the data (if not provided by 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.

Subject access requests can be submitted in any form, but are easier to record and process if made formally in writing. Requests should include:

- Name of individual
- Correspondence address, phone number and email
- Details of the information requested

Children and Subject Access Requests

Primary Schools

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/carers at primary schools will be granted without the express permission of the child. This is not a strict rule as a student's ability to understand their rights will always be judged on a case-by-case basis.

Secondary Schools

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/carers will not be granted without the express permission of the student. This is not a strict rule as a student'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, we:

- Ask the individual to provide two forms of identification (not applicable for student requests)
- Contact the individual by phone to confirm the request was made (not applicable for student requests)
- Will respond without delay and within one month of receipt of the request and confirmation of identity. This may extend to three months where a request is complex or numerous, with the individual being informed of this within 1 month and why the extension is necessary.
- Provide the information free of charge

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the student 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 we can't reasonably anonymise and we don't have the other person's consent and would be unreasonable to proceed without it.
- Is part of certain sensitive documents, such as those relating to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references or exam scripts.

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee which takes in to account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access rights through the courts.

Other Data Protection Rights of the Individual

In addition to the right to make a Subject Access Request, and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us 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
- Challenge decisions based solely on automated decision making or profiling, such as making decisions or evaluating aspects of an individual based on their personal data with no human involvement.
- 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).

Staff receiving a request 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 records of their child. However, the Trust may decide on a case-by-case basis to provide these. Requests to view an educational record must be submitted in writing by letter or email to the DPO. Requests should include:

- Name of individual
- Correspondence address, phone number and email
- Details of the information requested

Staff receiving a request must immediately forward it to the DPO.

Biometric Recognition Systems

Where we use students' biometric data as part of an automated biometric recognition system we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified in advance of the introduction of any biometric recognition system, and obtain written consent from at least one parent/carer before taking or processing any biometric data. They have the right to choose not to use biometric systems, and the school must provide alternative means of

accessing the relevant services for those students. Consent can be withdrawn at any time, with the school ensuring that any data already captured is deleted.

As required by law, if a student refuses to participate in or continue to participate in the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parents/carers.

We will also obtain the consent of staff or other persons prior to using school biometric systems, and provide alternative means of accessing the relevant service should they object. They can also withdraw consent at any time, with the school ensuring that any data already captured is deleted.

CCTV

CCTV is used in several schools to help improve safety and security, with all adhering to the ICO's code of practice. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded, with cameras clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should initially be directed to the Data Protection Officer, who will liaise directly with the individual school's premises team.

Photographs and Videos

We will obtain written consent from parents/carers of students up to and including Year 8 for photographs and videos to be taken of their child for communication, marketing and promotional purposes. We will explain how the photograph and/or video will be used to both the parent/carer and students. Consent is only required from the student in older year groups.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure that they cannot be identified.

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

Data Protection by Design and Default

The Trust has put measures in place to integrate data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain specialist 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.
- Completing Data Protection Impact Assessments where the 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, related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, related policies and any other data protection matters
- Regularly conducting reviews and audits to test our privacy measures to ensure we are compliant

- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws apply.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our schools and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - Maintaining an internal record of all personal data we hold, including type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and safeguards, retention periods and how we are keeping data secure

Data Security and Storage of Records

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

Main examples include:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are locked securely away when not in use
- Papers containing confidential personal data must not be left on office or classroom desks, staffroom tables, pinned to notice/display boards, or 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 school office
- Use of passwords that are at least 8 characters long containing letters and numbers to access school computers, laptops and other electronic devices. Staff and students 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. E-Mails containing any personal or sensitive data must be sent password protected or via end to end secure encryption (e.g. Galaxy key)
- Staff, students, Trustees or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Disposal of Records

The Trust will securely dispose of personal data that is no longer needed. Paper-based records will be shredded, with electronic records overwritten or deleted. Third party providers may also be used to safely dispose of records on the Trust's behalf. If so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Data Breaches

Any breach will be reported to the ICO within 72 hours, and made according to their 'Guidance on Personal Data Breaches, as follows:

Actions on Discovery of a Breach/Potential Breach

When a breach/potential breach is discovered, the staff member must immediately notify the DPO. The DPO will investigate 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 consider whether the breach must be reported to the ICO. In deciding, they 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) through:

- Loss of control over their data
- Discrimination
- Identity 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

Where the ICO is notified, the DPO will do this within 72 hours via the 'report a breach' page of the ICO website. If the DPO does not have full details of the incident, they will report as much detail as possible within this 72-hour period, explaining that there is a delay, reasons for the delay, and when the DPO expects to be able to provide this information. Once received, this remaining information will be submitted as soon as possible

The DPO will also assess the potential risk to individuals, based on the potential severity and likelihood of the breach. If the risk is high, the DPO will promptly inform all individuals in writing:

- The name and contact details of the DPO
- Likely consequences of the personal data breach
- Measures that have been, or will be, taken to deal with the breach to mitigate possible adverse effects

The DPO will coordinate all reasonable efforts to contain and minimise the impact of the breach. They will also meet with the Head of School and CEO to consider what measures can be put in place to prevent recurrence. Where relevant, the DPO will notify any relevant third parties who can help mitigate the loss to individuals such as police, insurers, banks or credit card providers.

Recording Data Breaches

The DPO will document all breaches, irrespective of whether they are reported to the ICO. This will include:

- Circumstances of the breach
- Effects
- Action taken to contain it and ensure it does not happen again

Records of all breaches will be stored electronically within the secure GDPR.CO.UK Site User area

Actions to Minimise the Impact of Data Breaches

The Trust will act to mitigate the impact of data breaches, focusing especially on breaches involving sensitive information. We will review the effectiveness of these actions and amend them as necessary following any 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. If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT department to recall it.
- Staff members who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- Where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explaining that the information was sent in error, and request that they 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, the DPO will contact the site to request that the information is removed and deleted.