CHELSEA ACADEMY

Anchored in Christ

Data Protection Policy

Approved by Governor committee:
Finance – 25th February 2019

Date to be reviewed:
February 2021

Responsibility of:
Data Protection Officer

Date ratified by Governing Board:
April 2019

Aims

Chelsea Academy (A Science Academy) aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data under the control of Chelsea Academy and its staff, regardless of whether it is in paper or electronic format.

Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our 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.

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more 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 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.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to personal data.

The data controller

Our Academy processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

The Academy is registered as a data controller with the ICO with number 71662808 and will renew this registration annually or as otherwise legally required.

Roles and responsibilities

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

Governing board

The governing board has overall responsibility for ensuring that our Academy 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 our compliance with data protection law and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on Academy data protection issues.

The DPO is also the first point of contact for individuals whose data the Academy processes and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Hannah Blake and is contactable via dpo@chelsea-academy.org

Principal

The Principal 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 of any changes to their own personal data and that they have collected, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - 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 GDPR is based on data protection principles that our Academy 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 aims to comply with these principles.

Collecting personal data

Lawfulness, fairness and transparency

We 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 can **fulfil a contract** with the individual, or the individual has asked the Academy to take specific steps before entering into a contract
- The data needs to be processed so that the Academy 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, 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 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 student) has freely given clear **consent**

For special categories of personal data we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals we will provide them with the relevant information required by data protection law.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it 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 order 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 Information and Records Management Society (IRMS) Retention Guidelines for Academies.

Sharing personal data

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

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

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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

Where we transfer personal data to a country or territory outside the European Economic Area, we 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 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, or if this is not possible, the criteria used to determine this period
- 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

Subject access requests must be submitted in writing, either by letter, or email to the DPO. They should 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 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 students at our Academy may not be granted without the express permission of the student. This is not a rule and 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:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- 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. We will inform the individual of this within 1 month and explain why the extension is necessary

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 child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into 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.

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 we are collecting their data about how we use and process it (see section 7), 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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- 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

Chelsea Academy will consider requests from parents to access to their child's educational record, in line with the provisions of the Education (Pupil Information) (England) Regulations 2005. This covers information that comes from a teacher or other employee of a local authority or school, the pupil or you as a parent, and is processed by or for the school's governing body or teacher, except for information the teacher has solely for their own use. We will respond to requests for access to the educational record within 15 days. There will

be no charge to view the educational record. We will charge for providing a copy of the educational record on a sliding scale from £1.20 for up to 19 pages, to £50 for over 500 pages.

To request access, please contact the Principal by email: principal@chelsea-academy.org

Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use fingerprints to receive Academy dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Academy will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the Academy's biometric system(s). We will provide alternative means of accessing the relevant services for those students.

Parents/carers and students can object to participation in the Academy's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant 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 parent(s)/carer(s).

Where staff members or other adults use the Academy's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the Academy will delete any relevant data already captured.

CCTV

We use CCTV in various locations around the Academy site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to seek the permission of the individual 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 Lucian Boyd Harte, Director of Finance and Operations.

Photographs and videos

As part of our Academy activities, we may take photographs and record images of individuals within the Academy.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Uses may include:

- Within the Academy on notice boards and in Academy magazines, brochures, newsletters, etc.

- Outside of the Academy by external agencies such as the Academy photographer, newspapers, campaigns
- Online on our Academy website or social media pages

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 they cannot be identified.

Data protection by design and default

We will put measures in place to show that we have integrated 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 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 Data Protection Impact Assessments (DPIA) where the Academy'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; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Academy and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Data security and storage of records

We 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 sensitive personal data must not be left on office and classroom desks, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access Academy computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals

- Electronic documents containing sensitive personal data are password protected or shared used Google permissions.
- Encryption software is used to protect all portable devices, USB's memory devices are barred from use and blocked.
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for Academy-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 (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 we cannot or do not need to rectify or update it.

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

Personal data breaches

The Academy will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

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

- A non-anonymised dataset being published on the Academy website which shows the exam results of students eligible for the student premium
- Safeguarding information being made available to an unauthorised person
- The theft of an Academy laptop containing non-encrypted personal data about students

Training

All staff and governors 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's processes make it necessary.

Appendix 1: Personal data breach procedure

Step 1: Log, validate, acknowledge, evaluate

- A breach is identified
- The following information must be emailed to the DPO via the Academy data protection email address:
    a. Name of individual reporting, and contact details
    b. Date and time of the breach or incident
    c. Details of the incident (what has happened and when / how the breach was identified)
    d. Type of data e.g. names, medical information
    e. Number and category of individuals affected (if known) e.g. students, staff, parents
- DPO will evaluate the incident and contact 9ine consulting for support where necessary

Step 2: Evaluate and act

- DPO, and where appropriate 9ine consulting, will review the breach incident impact evaluation and the outcome of the assessment will be a classification of:

  Level 0 No breach/near miss

  Level 1: (minor) Which can be dealt with internally by the Academy. No data incident investigation meeting is require. The DPO will keep the highest level of Academy management aware of progress.

  Level 2 (potentially serious): Which may be reported to the supervisory authority, based on the outcome of SIRI

  Level 3 (serious): reportable to ICO

- Where classed as a Level 3, DPO will convene a Data Incident Investigation meeting, providing an agenda and expected outcomes. The meeting is required within 72 hours of the breach being identified.
- Where classed as a Level 0 or 1 or 2, the DPO will log the incident and evaluate remedial action given the nature of the incident.

- The Academy will inform 9ine of the outcome of the Data Incident Investigation meeting. The Academy will provide the necessary resources to mitigate the breach and action immediately.

- Where reportable to the supervisory authority, DPO will make contact with the supervisory authority to determine whether the breach will be investigated.

Step 4: Containment and recovery

- Minutes from the Data Incident Investigation Meeting will be recorded and the necessary resources allocated by the Academy to mitigate the impact of the breach
- The DPO will manage the completion of the actions, documenting the actions taken and consequential impact on risks to the rights and freedoms of natural persons.

Step 5: Assessment of ongoing risk

- The DPO will continually evaluate the progress of actions taken to mitigate the impact on natural persons. Where necessary, they will request 9ine consulting to provide advice and guidance on the proportionality of the Academy's response, provision of necessary resources and progress.

Step 6: Notification of breach

- The DPO will allocate responsibility for communications to a nominated individual. They will be responsible for managing the breach communication to affected individuals. The nominated individual will notify affected individuals without undue delay of the breach, the impact of the breach on the security of their personal information, possible risks and actions they should take.

Step 7: Evaluation and response

- Within 14 days of the breach occuring, 9ine will issue the DPO with a post-breach evaluation template and checklist.
- The DPO will complete the post-breach evaluation and submit to 9ine.

Data Incident Investigation Meeting Structure and Guidelines

Membership

In the case of Level 3 incidents the membership will consist of:

- Principal of the Academy
- Director of Financial Operations of the Academy
- DPO

For network related breaches:

- IT Network Manager of the Academy

Notification of the meeting, agenda, minutes and actions will be sent to:

- Chair of Governors
- Governor Data Protection Representative
- 9ine Consulting

Meeting Agenda

The meeting should be structured around the following agenda:

- Detail of the date, time and location of the incident
- Description of what has happened e.g:
    - Theft, accidental loss, inappropriate disclosure, procedural failure etc
- The number and types of data subjects involved e.g:
    - Staff, students, parents
- The number of records involved
- The format of the records (paper or digital)
- Description of the security protections that were in place e.g:
    - Encryption
    - Lockable bag / cabinet / room
- The type of records or data involved
- Who has been formally and informally notified
- The potential risks to the rights and freedoms of natural persons

- The mitigation actions that should be taken to mitigate those risks
- The provision of 'necessary' resources to contain and manage the breach e.g:
    - Legal
    - HR
    - IT
    - Cyber
    - Data protection
- Communications plan
- Summary of actions
- Next meeting

Records of all breaches will be stored in the Google GDPR folder.

- The DPO and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.