Data Protection

Approved by Directors:	**March 2026**
Review date:	**March 2027**
DIRECTOR LEAD	**Ben Cox**

POLICY STATEMENT

The purpose of this policy is to set out the standards on how eCAPH will store and process personal data in accordance with UK data protection law.

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
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

DEFINITIONS

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living 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 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.

THE DATA CONTROLLER

eCAPH processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

eCAPH is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

ROLE AND RESPONSIBILITIES

Exec Board & Directors

The Executive Board/Directors have overall responsibility for ensuring that eCAPH complies with all relevant data protection obligations.

Data Protection Officer (DPO)

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.

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

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

Our DPO is eCAPH Business Manager and is contactable via businessmanager@ecaph.org

DATA PROTECTION PRINCIPALS

The UK GDPR is based on data protection principles that eCAPH 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 eCAPH aims to comply with these principles.

COLLECTING PERSONAL DATA

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.

Personal data must only be processed where it is necessary in order to do their jobs.

Data will be accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when eCAPH no longer need the personal data they hold, they must ensure it is deleted or anonymised.

SHARING PERSONAL DATA

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- We need to liaise with other agencies – we 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, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor 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

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

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 staff, delegates or suppliers.

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

SUBJECT ACCESS REQUESTS

When responding to requests, eCAPH will:

- 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 (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. We will inform the individual of this within 1 month, and explain why the extension is necessary.
- We may not disclose information for a variety of reasons, such as if it:
- Might cause serious harm to the physical or mental health of an individual
- Would include another person's personal data that we can't reasonably anonymise, and we don't 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, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

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 right through the courts.

Data Protection Rights

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 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 that has been justified on the basis of public interest, official authority or legitimate interests.
- Challenge decisions based solely on automated decision making or profiling i.e. making decisions or evaluating certain things about 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).
- 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.
-

DATA SECURITY AND STORAGE OF RECORDS

eCAPH 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 anywhere where there is general access.
- Passwords that are at least 10 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff are reminded that they should not reuse passwords from other sites.
- 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.

PERSONAL DATA BREACHES

eCAPH 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 guidance on personal data breaches

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it.

MONITORING ARRANGEMENT

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the Exec Board/Directors.