Update: April 2026

Cornerstone Academy Trust

Data Protection Policy

Cornerstone Academy Trust - Policy Statement

Data Protection Policy

This policy in drafted in accordance with the requirements of the General Data Protection Regulation ("**GDPR**") and should be read in conjunction with our privacy notices.

Definitions

Term	Definition
Data	is information, which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Personal Data Breach	A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our workforce (including Trustees and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available,

	alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data. Please refer to our Protection of Biometric Information Policy for more detail.
Workforce	Includes, any individual employed by the Trust such as staff and those who volunteer in any capacity including Trustees/Members/parent helpers

Policy statement

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as a Trust, we will collect, store and process personal data about our pupils, workforce, parents and others. This makes us a data controller in relation to that personal data.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

We are committed to the protection of all personal data and special category personal data for which we are the data controller.

The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

About this policy

This policy sets out the Cornerstone Academy Trust commitment to handling personal data in line with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, Data (Use and Access) Act 2025 and associated laws governing the processing of personal data in the UK (hereafter known as 'data protection legislation').

The Trust is the data controller for the personal data it processes and is registered with the Information Commissioner's Office (ICO) under registration number Z2454183. Details about this registration can be found at www.ico.org.uk

The purpose of this policy is to explain how the Trust handles personal data under data protection legislation and is to inform staff and other individuals who process personal data on the Trust's behalf of the Trust's expectations.

Scope

This policy applies to the processing of personal data held by the Trust as defined by Article 4 of the UK GDPR, and to the processing of special categories of personal data defined by Article 9 of the UK GDPR.

This includes personal data held about pupils, parents/carers, staff, temporary staff, governors, visitors, and any other identifiable data subjects.

This policy should be read alongside the:

- Internet Safety Policy
- Subject Access Request Policy
- Acceptable Use Agreements
- Records of Retention Policy and Schedule
- Protection of Biometrics Policy
- Social Media Policy
- AI Policy

Roles and Responsibilities

Trustees:

The Trustees have overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

Executive Headteacher:

The Executive Headteacher has day-to-day responsibility for ensuring this policy is adopted and adhered to by staff and other individuals processing personal data on the Trust's behalf.

Data Protection Officer:

As a Trust we are required to appoint a Data Protection Officer (**"DPO**").

The Data Protection Officer (DPO) is responsible for carrying out the tasks set out in Article 39 of the UK GDPR. In summary, the DPO is responsible for:

- Informing and advising the Trust of their obligations under the data protection legislation.
- Monitoring compliance with data protection policies.
- Raising awareness and delivering training to staff.
- Carrying out audits on the Trust's processing activities.
- Providing advice regarding Data Protection Impact Assessments and ensuring these are reviewed annually.
- Co-operating with the Information Commissioner's Office.
- Acting as the contact point for data subjects exercising their rights.

The DPO is also the central point of contact for all data subjects and others in relation to matters of data protection.

Our DPO is Jenny Goodall, and our DPLO is Kyriaki Constanti they can be contacted via DPO@tcat.education

Staff, temporary staff, contractors, visitors

All staff, temporary staff, contractors, visitors, and other individuals processing personal data on behalf of the Trust, are responsible for complying with the contents of this policy.

- All individuals shall remain subject to the common law duty of confidentiality when their employment or relationship with the Trust ends. This does not affect an individual's rights in relation to whistleblowing.
- Failure to comply with this policy may result in disciplinary action or termination of employment or service contract.
- All individuals handling the Trust's data shall be made aware that unauthorised access, use or sharing of data, may constitute a criminal offence under the Data Protection Act 2018 and/or the Computer Misuse Act 1990.

Policy Content

Data protection principles

Anyone processing personal data must comply with the data protection principles. These provide that personal data must be:

- Processed fairly and lawfully and transparently in relation to the data subject;
- Processed for specified, lawful purposes and in a way, which is not incompatible with those purposes;
- Adequate, relevant and not excessive for the purpose;
- Accurate and up to date;
- Not kept for any longer than is necessary for the purpose; and
- Processed securely using appropriate technical and organisational measures.

The Trust and all individuals processing personal data controlled by the Trust, shall comply with these principles.

The Trust shall have appropriate measures and records in place to demonstrate compliance with each of the principles ('accountability').

Personal Data must also:

- be processed in line with data subjects' rights;
- not be transferred to people or organisations situated in other countries without adequate protection.

We will comply with these principles in relation to any processing of personal data by the Trust.

Fair and lawful processing

Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed fairly, data subjects must be made aware:

- that the personal data is being processed;
- why the personal data is being processed;
- what the lawful basis is for that processing (see below);
- whether the personal data will be shared, and if so with whom;
- the period for which the personal data will be held;
- the existence of the data subject's rights in relation to the processing of that personal data; and

- the right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing.

We will only obtain such personal data as is necessary and relevant to the purpose for which it was gathered and will ensure that we have a lawful basis for any processing.

For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally process personal data under the following legal grounds:

- where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract;
- where the processing is necessary to comply with a legal obligation that we are subject to, (e.g. the **Education Act 2011**);
- where the law otherwise allows us to process the personal data or we are carrying out a task in the public interest; and
- where none of the above apply then we will seek the consent of the data subject to the processing of their personal data.

When special category personal data is being processed then an additional legal ground must apply to that processing. We will normally only process special category personal data under following legal grounds:

- where the processing is necessary for employment law purposes, for example in relation to sickness absence;
- where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
- where the processing is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and
- where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data.

We will inform data subjects of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

If any data user is in doubt as to whether they can use any personal data for any purpose, then they must contact the DPO before doing so.

Vital Interests

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

Most of the Trust's processing of personal data will not require consent from data subjects (or their parents/carers as appropriate), as the Trust needs to process this data in order to carry out its official tasks and public duties as a Trust.

- However, there are circumstances when the Trust is required to obtain consent to process personal data, for example:
- To collect and use biometric information (such as fingerprints or facial recognition) for identification purposes.
- To send direct marketing or fundraising information by email or text where the data subject would not have a reasonable expectation that their data would be used in this way or have objected to this.
- To take and use photographs, digital or video images and displaying, publishing, or sharing these in a public arena such as:
- on social media;
- in the Trust prospectus;
- on the Trust website;
- in the press/media;
- in the Trust newsletter

To share personal data with third parties (for example professionals, agencies, or organisations) where the data subject has a genuine choice as to whether their data will be shared, for example when offering services which the data subject does not have to accept or agree to receive.

When the Trust relies on consent as its lawful basis, it will ensure that the following requirements are met:

- The consent is freely given
- The person giving consent is fully informed and fully understands what they are consenting to and any non-obvious consequences of giving or refusing consent

There must be a positive indication of consent (opt-in as opposed to opt-out), and consent shall not be assumed as being given if no response has been received.

The person giving their consent will be able to withdraw their consent at any time.

Consent shall be documented so that it may be evidenced and referred to in the future, if necessary.

Where consent is being obtained for the collection or use of children's information, consent shall be obtained from a parent or guardian until the child is considered to have sufficient maturity to make the decision themselves (except where this is not in the best interests of the child. In such cases, consent will be obtained from an adult with parental responsibility for that child).

The Trust shall ensure that where consent is obtained, there is a record of this. Where possible, consent shall be obtained in writing. All forms requesting consent shall include a statement informing the person of their right to withdraw, and an email address so they may notify the Trust of any changes or withdrawal of consent.

Processing for limited purposes

In the course of our activities as a Trust, we may collect and process the personal data set out in our record of processing activities (RoPA). This may include personal data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or

otherwise) and personal data we receive from other sources (including, for example, local authorities, other Trusts, parents, other pupils or members of our workforce).

We will only process personal data for the specific purposes set out in our RoPA or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

The Trust shall not process data in any way which would be incompatible with these purposes.

Notifying data subjects

If we collect personal data directly from data subjects, we will inform them about:

- our identity and contact details as Data Controller and those of the DPO;
- the purpose or purposes and legal basis for which we intend to process that personal data;
- the types of third parties, if any, with which we will share or to which we will disclose that personal data;
- whether the personal data will be transferred outside the European Economic Area ('**EEA**') and if so the safeguards in place;
- the period for which their personal data will be stored, by reference to our Retention and Destruction Policy;
- the existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making; and
- the rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

Unless we have already informed data subjects that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive personal data about a data subject from other sources, we will provide the data subject with the above information as soon as possible, thereafter, informing them of where the personal data was obtained from.

Adequate, relevant and non-excessive processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject, unless otherwise permitted by Data Protection Legislation.

Accurate data

1. The Trust shall take all reasonable efforts to ensure the personal data it holds is accurate and where necessary kept up to date. Where personal data is found to be inaccurate, this information will be corrected or erased without delay.
2. The Trust will send frequent reminders, on at least an annual basis, to parents/carers, pupils, and staff, to remind them to notify the Trust of any changes to their contact details or other information.
3. The Trust shall carry out sample checks of pupil and employee files containing personal data, to ensure the data is accurate and up to date. This will be carried out on an annual basis.

Storage limitation and disposal of data

The Trust shall keep personal data for no longer than is necessary for the purpose(s) of the processing. The Trust shall maintain and follow a Record Retention Schedule [insert link], which sets out the

timeframes for retaining personal data. This schedule shall be published alongside the Trust's privacy notices on the website.

The Trust shall designate responsibility for record disposal/deletion to nominated staff, who shall adhere to the Trust's Record Retention Schedule Document-Retention-Policy-Feb-26-1.pdf and ensure the timely and secure disposal of the data.

Security of Personal Data

The Trust shall have appropriate security in place to protect personal data against unauthorised or accidental access, disclosure, loss, destruction, or damage. This will be achieved by implementing appropriate technical and organisational security measures.

Technical security measures

- The Trust shall implement proportionate security measures to protect its network and equipment and the data they contain. This includes, but is not limited to:
- having a Firewall, anti-virus, and anti-malware software in place
- applying security patches promptly
- restricting access to systems on a 'need to know' basis
- enforcing strong password policies; passwords shall be a minimum of 8 characters in length; changed at appropriate intervals and not shared or used by others
- the use of 2FA or MFA (2 Factor Authentication / Multi-Factor Authentication) wherever possible, and particularly on accounts which access / contain special category or sensitive personal data
- encrypting laptops, mobile phones, USBs and other portable devices or removable media containing personal data
- regularly backing up data
- regularly testing the Trust's disaster recovery and business continuity plans, to ensure data can be restored in a timely manner in the event of an incident

Organisational security measures

- The Trust will ensure the following additional measures are also in place to protect personal data:
- Staff shall sign confidentiality clauses as part of their employment contract
- Data protection awareness training shall be provided to staff during induction and bi-annually thereafter
- Cyber security training, guidance or advice shall be provided to staff on a regular basis
- Policies and guidance shall be in place relating to the handling of personal data whilst during and outside of Trust. These will be communicated to staff and other individuals as necessary, including policy revisions. A policy declaration shall be signed by staff and retained on their personnel file.
- Data protection compliance shall be a regular agenda item in governing body and Senior Leadership Team meetings.
- Cross cutting shredders and/or confidential waste containers will be available on the Trust's premises and used to dispose of paperwork containing personal data.
- Appropriate equipment and guidance will be available for staff to use and follow when carrying paperwork off Trust premises.
- The Trust's buildings, offices and where appropriate classrooms, shall be locked when not in use.

- Paper documents and files containing personal data shall be locked in cabinets/cupboards when not in use, and access restricted on a need to know basis.
- Procedures shall be in place for visitors coming onto the Trust's premises. These will include signing in and out at reception, wearing a visitor's badge and being escorted by a Trust employee (unless the visitor holds a valid Disclosure and Barring Service certificate, or it is otherwise appropriate for the person not to be escorted).

The Trust shall have procedures in place to identify, report, record, investigate and manage personal data breaches in the event of a security incident.

Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

Processing in line with data subject's rights

Data subjects have several rights under data protection legislation. The Trust shall comply with all written requests from data subjects exercising their rights without delay, and within one month at the latest, although we do have the right to extent this deadline by a further two calendar months for requests considered to be complex.

We will process all personal data in line with data subjects' rights, in particular their right to:

- request access to any personal data we hold about them;
- object to the processing of their personal data, including the right to object to direct marketing;
- have inaccurate or incomplete personal data about them rectified;
- restrict processing of their personal data;
- have personal data we hold about them erased;
- have their personal data transferred; and
- object to the making of decisions about them by automated means.

The Right of Access to Personal Data

Data subjects may request access to all personal data we hold about them. Such requests will be considered in line with the Trusts Subject Access Request Policy

The Right to Object

In certain circumstances data subjects may object to us processing their personal data. This right may be exercised in relation to processing that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

An objection to processing does not have to be complied with where the Trust can demonstrate compelling legitimate grounds which override the rights of the data subject.

Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

In respect of direct marketing any objection to processing must be complied with.

The Trust is not however obliged to comply with a request where the personal data is required in relation to any claim or legal proceedings.

The Right to Rectification

If a data subject informs the Trust that personal data held about them by the Trust is inaccurate or incomplete, then we will consider that request and provide a response within one month.

If we consider the issue to be too complex to resolve within that period, then we may extend the response period by a further two months. If this is necessary, then we will inform the data subject within one month of their request that this is the case.

We may determine that any changes proposed by the data subject should not be made. If this is the case, then we will explain to the data subject why this is the case. In those circumstances we will inform the data subject of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

Data subjects have a right to "block" or suppress the processing of personal data. This means that the Trust can continue to hold the personal data but not do anything else with it.

The Trust must restrict the processing of personal data:

- Where it is in the process of considering a request for personal data to be rectified (see above);
- Where the Trust is in the process of considering an objection to processing by a data subject;
- Where the processing is unlawful, but the data subject has asked the Trust not to delete the personal data; and
- Where the Trust no longer needs the personal data, but the data subject has asked the Trust not to delete the personal data because they need it in relation to a legal claim, including any potential claim against the Trust.

If the Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

Data subjects have a right to have personal data about them held by the Trust erased only in the following circumstances:

- Where the personal data is no longer necessary for the purpose for which it was originally collected;
- When a data subject withdraws consent – which will apply only where the Trust is relying on the individuals consent to the processing in the first place;
- When a data subject objects to the processing and there is no overriding legitimate interest to continue that processing – see above in relation to the right to object;
- Where the processing of the personal data is otherwise unlawful; and
- When it is necessary to erase the personal data to comply with a legal obligation.

The Trust is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:

- To exercise the right of freedom of expression or information;
- To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;
- For public health purposes in the public interest;
- For archiving purposes in the public interest, research or statistical purposes; or
- In relation to a legal claim.

If the Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

The DPO must be consulted in relation to requests under this right.

Right to Data Portability

In limited circumstances a data subject has a right to receive their personal data in a machine-readable format, and to have this transferred to another organisation.

If such a request is made, then the DPO must be consulted.

Data protection by design and default

The Trust shall have appropriate technical and organisational measures in place which are designed to implement the data protection principles in an effective manner, and will ensure that by default, it will only process personal data where it is necessary to do so. The Trust's Data Protection Policy and supplementary policies, procedures and guides, explain how the Trust aims to achieve this.

Joint controller agreements

The Trust shall sign up to agreements with other data controllers where personal data is shared or otherwise processed on a regular basis, where it is necessary to do so.

Data processors

The Trust shall carry out checks with prospective data processors (e.g. suppliers providing goods or services which involve the processing of personal data on the Trust's behalf) to assess they have appropriate technical and organisational measures that are sufficient to implement the requirements of the data protection legislation and to protect the rights of data subjects.

The appropriateness of data processors will be assessed by the Trust and the Data Protection Officer before the Trust purchase the service. A record will be kept of their findings.

The Trust shall ensure there are appropriate written contracts/Terms of Service in place with data processors, which contain the relevant clauses listed in Article 28 of the UK GDPR.

Record of Processing Activities (RoPA)

The Trust shall maintain a record of its processing activities in line with Article 30 of the UK GDPR. This inventory shall contain the following information:

- Name and contact details of the Trust and its Data Protection Officer
- Description of the personal data being processed

- Categories of data subjects
- Purposes of the processing and any recipients of the data
- Information regarding any overseas data transfers and the safeguards around this
- Retention period for holding the data
- General description of the security in place to protect the data
- This inventory shall be made available to the Information Commissioner upon request.

Management of personal data breaches

The Trust shall have procedures in place to identify, report, record, investigate and manage personal data breaches (i.e. security incidents involving personal data). These include security incidents resulting in the:

- unauthorised or accidental disclosure or access to personal data (breach of confidentiality)
- unauthorised or accidental alteration of personal data (breach of integrity)
- accidental or unauthorised loss of access or destruction of personal data (breach of availability)

All security incidents and suspected personal data breaches must be reported to the Data Protection Officer immediately, via the Trust's Data Protection Link Officer, by emailing DPO@tcat.education

All incidents will be recorded in the Trust's data breach log and investigated by a member of the Senior Leadership Team (or other person as appropriate), under the support and direction of the Trust's Data Protection Officer.

Notification to the ICO and Data Subjects

The Data Protection Officer shall determine whether the Trust must notify the Information Commissioner's Office and data subjects.

Where a breach is likely to result in a risk to the data subject, for example if they could suffer damage, discrimination, disadvantage or distress as a result of the breach, the Trust (or the Data Protection Officer) shall notify the Information Commissioner's Office (ICO) within 72hrs of becoming aware of the breach.

If the breach is likely to result in 'high risks' to data subjects, for example if the breach could lead to identity theft, psychological distress, humiliation, reputational damage or physical harm, the Trust shall inform the data subject promptly and without delay.

When informing a data subject of a personal data breach involving their personal data, the Trust shall provide in clear, plain language the:

- nature of the incident
- name and contact details of the Data Protection Officer
- likely consequences of the breach
- actions taken so far to mitigate possible adverse effects

Data Protection Impact Assessments

The Trust shall carry out Data Protection Impact Assessments (DPIAs) on all processing of personal data, where this is likely to result in high risks to the rights and freedoms of data subjects, particularly when using new technologies. This includes, but is not limited to the following activities:

- Installing and using Closed Circuit Television (CCTV)
- Collecting and using biometric information, such as fingerprints
- Any sharing of special category data with other organisations
- Using mobile Applications to collect or store personal data, particularly about children
- Any storing / processing of special category data
- Use of Artificial Intelligence applications
- Using systems that record large volumes of personal data, particularly where data processors are involved

The results from DPIAs shall be recorded and shared with the Data Protection Officer, who will advise on any privacy risks and mitigations that can be made to reduce the likelihood of these risks materialising. The Data Protection Officer will monitor the outcome of the DPIA, to ensure the mitigations are put in place and that DPIA's are reviewed annually.

Disclosure and sharing of personal information

The Trust shall adhere to statutory and non-statutory guidance around sharing personal data as set out in the following:

When sharing personal data with third parties the Trust shall adhere to the following principles:

Keeping Children Safe in Education (DfE 2024)
10 Step Guide to sharing information to safeguard children (ICO)
Data Sharing Code of Practice (ICO 2020)
DfE Information Sharing Advice for Practitioners providing safeguarding services to children, young…

Data subject(s) shall be made aware of the sharing through privacy notices or specific communications regarding the sharing

- Identification of an appropriate lawful basis prior to sharing data
- Data shared shall be adequate, relevant and limited to what is necessary
- Accuracy of the data shall be checked prior to the sharing (where possible)
- Expectations regarding data retention shall be communicated
- Data shall be shared by secure means and measures in place to protect the data when received by the third party
- A record shall be kept of the data sharing

The Trust recognises that the data protection laws allow organisations to share necessary personal data with third parties to protect the safety or well-being of a child and in urgent or emergency situations to prevent loss of life or serious physical, emotional or mental harm and this is included in the Trust's data protection training for all staff.

Data Processors

We contract with various organisations who provide services to the Trust, including payroll providers, project managers, accountancy and legal professionals, and third-party application providers (e.g. payment modules, communication modules) among others.

In order that these services can be provided effectively we are required to transfer personal data of data subjects to these data processors.

Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The Trust will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

Contracts with data processors will comply with Data Protection Legislation and contain explicit obligations on the data processor to ensure compliance with the Data Protection Legislation, and compliance with the rights of Data Subjects.

Images and Videos

Parents and others attending Trust events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a Trust performance involving their child. The Trust does not prohibit this as a matter of policy.

The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to prevent.

The Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

As a Trust we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering Trust events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

Whenever a pupil begins their attendance at the Trust, they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil.

CCTV

The Trust operates a CCTV system which is managed in line with our CCTV Policy.

Your right to complain

We work to high standards when it comes to processing your personal information. We hope you will always be happy with the way we handle your information, however if we have not met your expectations, please let us know so we can put things right. To make a complaint, please complete our Data Protection Complaints Form, available on our website or directly via the link below:

Data Protection Complaints Form - The Cornerstone Academy Trust

Changes to this policy

We may change this policy at any time. Where appropriate, we will notify data subjects of those changes.

Updates to this Policy

Reviewed by (job role):	**Date:**	**Next Review Date:**

Full Trust Board	September 2023	September 2025
DPO/DPLO	April 2026	April 2028