Lincolnshire Gateway Academies Trust

Data Protection Policy

Date reviewed:	**September 2025**	
Approved by:	**CEO**	**October 2025**
Next review due by:	**September 2026**	

For Office Use Only:

Policy Version: 1.3

To make changes to this policy, please email admin@lincolnshiregateway.co.uk.

Introduction

Lincolnshire Gateway Academies Trust (the Trust) collects and uses personal information about staff, students, parents[1] and other individuals and organisations that come into contact with it. This information is essential to the running of the Trust and its constituent academies. The Trust also makes use of CCTV to protect its staff and students in addition to its grounds and other property.

Unlike other companies, the Trust has a legal requirement detailed in our privacy notices to gather information about staff, students and their families in order to ensure that it is fully compliant with statutory requirements and it is vital that the trust relationship between the Trust and its employees, students and their parents is strong. The aim of this policy is to set out what the Trust's policies and procedures are to prevent the possibility of data breaches as well as providing guidance on specific types of data and their collection and storage.

The Trust is committed to the security and integrity of the personal and sensitive data that it is required to hold and takes its responsibility as a data controller seriously, this policy aims to ensure that all staff are aware of their responsibilities with regards to compliance with the Data Protection Act and its principles.[2]

Aims & Scope

The Trust aims to ensure that all data collected about staff, pupils, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation EU 2016/679 (GDPR)[3] as it stood on 31 December 2020 and the Data Protection Act 2018 (DPA 2018)[4]. It also complies with our funding agreement and articles of association.

This policy applies to all Trust and constituent academy staff, the majority of whom will process sensitive data on a regular basis through mark books, student data systems and their own individual or departmental tracking systems and covers data both held within the Trust and held on secure, approved systems outside of the Trust.

Legislation & Guidance

This policy meets the requirements of the GDPR and DPA 2018 and utilises guidance published by the Information Commissioner's Office (ICO) on the GDPR[5]. It also meets the requirements of the Protection of Freedoms Act 2012[6] with regards to usage of biometric data. The Trust also follows the ICO Code of Practice[7] with regards to its CCTV usage.

[1] "parents" in the case of this document refers to adults with parental responsibility
[2] https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX:02016R0679-20160504
[4] http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
[5] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
[6] https://www.legislation.gov.uk/ukpga/2012/9/part/1/chapter/2
[7] https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, living individual. This may include the individual's name, identification number, location data, online identifier or other factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.
Special Category Personal Data	Personal data which is more sensitive and needs more protection, including information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics, health – both physical and 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. This 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 their behalf. Lincolnshire Gateway Academies Trust serves as the Data Controller for itself and its constituent academies.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Responsible Persons

Governing Board

The governing board have overall responsibility for ensuring that The Trust and its constituent academies comply with all relevant data protection obligations.

Data Protection Officer

The Trust's Data Protection Officer (DPO)[8] is responsible for ensuring that the governing board is kept up to date with data protection risks & responsibilities. They also will perform regular reviews of data protection policies within the Trust and update them as necessary, as well as ensuring appropriate training is organised where required.

The DPO is also responsible for coordinating the response to Freedom of Information requests, Subject Access requests and Data Breaches, and ensuring that data provided to relevant parties is accurate and complies fully with both the request and the law.

[8] "Data Protection Officer" here is synonymous with Data Controller

The DPO is responsible for the implementation and maintenance of this document and in ensuring the Trust's compliance with the relevant statutes. This includes maintaining an Information Asset Register, performing regular Data Audits, conducting Privacy Impact Assessments and ensuring that our other policies and procedures remain current and in step with any changes to the law.

Each of the Trust's constituent academies has a dedicated Data Protection Officer with a lead officer operating within the Trust to provide advice and guidance.

Information and Communications Systems Officer

The ICS Officer is responsible for ensuring (with the cooperation of the DPO) that software and other systems used within the Trust are appropriate and adequately secure and should research systems being considered for use whilst considering the obligations of the Trust with regards to security as a priority.

Marketing and Recruitment

Staff responsible for Marketing and Recruitment must ensure that any outward contact from the Trust to prospective staff, students and their families is compliant with Data Protection legislation including statements attached to external emails and any other marketing copy. The Academy Principal should be the first point of contact for external agencies requesting information and should ensure that they conduct their due diligence before the external agencies are directed to the correct person.

All Staff

Staff are responsible for the collection, storage and processing of data in accordance with this policy. Keeping the Trust and/or academy informed of changes to personal data. Staff are responsible for contacting the Data Protection Officer if they have any concerns, questions or to report a breach.

Data protection principles

The Data Protection Act is based on data protection principles that the Trust 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 Trust 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 Trust can fulfil a contract with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the Trust can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the Trust, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the Trust (where the processing is not for any tasks the Trust performs as a public authority) 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 pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

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

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

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

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

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.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when 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 Trust's record retention schedule.

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:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- 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 which can provide sufficient guarantees that they comply with 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 pupils or staff.

Where we transfer personal data internationally, 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 or Trust holds about them. Please refer to the Subject Access Request Policy for more information.

Automated Processing

The Trust does not make sole use of automated processing for the purposes of decision making or profiling.

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 (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 (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

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.

Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school 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 pupils have the right to choose not to use the academies' biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners using a PIN number for identification rather than their thumb print.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil 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 pupil's parent(s)/carer(s).

Where staff members or other adults use the academies' 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 Trust and/or academy will delete any relevant data already captured.

CCTV

We use CCTV in various locations around the academy sites 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 ask individuals' permission 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 the Data Protection Officer. For further information about how the Trust utilises CCTV, please refer to our CCTV Policy.

Photographs and videos

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

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils 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 pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Whilst discouraged, any photographs and videos taken by parents/carers at academy events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the Trust or constituent academies take photographs and videos for marketing purposes, uses may include:

- Within academies on notice boards and in academy magazines, brochures, newsletters, etc.
- Outside of the academy by external agencies such as the Trust/academy photographer, newspapers, campaigns
- Online on our Trust or academy websites 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.

Online and Remote Learning

The Trust takes advantage of Remote Learning resources, such as Microsoft Teams as a part of Office 365 to provide access to education to learners when the academy premises are closed during normal operations.

The data we share with such services is only what is necessary to provide a functional service and is automatically removed upon the closure of a computer account and all files deleted.

Files uploaded to Office 365 or its services using an account provided by the Trust are considered property of the Trust for Data Protection, Safeguarding and other purposes. The Acceptable Use Policy applies to all files, messages and communications shared or uploaded to online learning platforms.

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
- Completing data protection impact assessments where the Trust and/or 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of our processing activities, including:

- For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, 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. For more information about how the Trust works to keep data secure, please refer to the Acceptable Use Policy.

ICS Staff may ask for personal details to confirm a user's identity on receipt of a password reset request.

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.

For further information about the disposal of data, please refer to our Data Retention Policy.

Personal data breaches

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

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. The Academy or the Trust, as applicable, must retain records of data breaches in accordance with the Data Retention policy regardless of whether a breach is reported to the ICO.