

LANCASTER ROYAL GRAMMAR SCHOOL

POLICY STATEMENT

Number 39	Date Approved By Trust Board July 2026
----------------------------	---

DATA PROTECTION POLICY

The Trust Board of Lancaster Royal Grammar School has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with education regulations and all other statutory provisions.

The Headmaster and Trustees of Lancaster Royal Grammar School have to comply fully with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1998. The Data Protection Act 2018 is now in force and encompasses the EU's GDPR (General Data Protection Regulations). The GDPR came into force from 25th May 2018. Having left the EU this ceased to apply after 31st December 2020. However, the UK's DPA 2018 had already enacted the EU GDPR's requirements into UK law and, with effect from 1 January 2021, the DPPEC (Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit)) Regulations 2019 amended the DPA 2018 and merged it with the requirements of the EU GDPR to form a new, UK-specific data protection regime that works in a UK context after Brexit as part of the DPA 2018.

This new regime is known as the 'UK GDPR'.

All staff involved with the collection, processing and disclosure of personal data are to be aware of their duties and responsibilities by these guidelines.

Guiding Principles – UK GDPR

The following is a summary of UK GDPR and provides the guiding principles upon which this policy is based.

Data must be

1. Processed in a fair, lawful and transparent manner
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and where necessary kept up to date (inaccurate data should be erased or rectified without delay)

5. Kept in a form permitting identification for no longer than is necessary
6. Processed in a manner ensuring appropriate security of the personal data

Enquiries

Information about Lancaster Royal Grammar School's Data Protection Policy is available from the Headmaster. General information about UK GDPR can be obtained from the Data Protection Commissioner (information line 01625 545 745, website www.dataprotection.gov.uk).

Fair obtaining and processing

Lancaster Royal Grammar School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

"Data" are tokens that can be interpreted as some kind of value, usually either as a quantitative measurement of or a qualitative fact about something. Biometrics and CCTV images are examples of data processed by the school.

"Processing," means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.

"Data subject" means an individual who is the subject of personal data or the person to whom the information relates.

"Personal data" means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.

"Parent" has the meaning given in the education act 1996 and includes any person having parental responsibility or care of a child.

Registered purposes

The data protection register entries for the school are available for inspection, by appointment, at the school office. Explanation of any codes and categories entered is available from the Head of Boarding who is the person nominated to deal with data protection issues in the school. Registered purposes covering the data held at the school are listed on the school's registration and data collection

documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

Data integrity

The school undertakes to ensure data integrity by the following methods:

Data accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the school of a change of circumstances, their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the school will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Trust Board for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data adequacy and relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the school will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. The Head of Boarding will carry out a termly check for irrelevant data and ensure that the records are amended as appropriate.

Length of time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Head of Boarding to ensure that obsolete data are properly erased. We follow the Lancashire County Council data retention schedule except for pupil data which we were told to retain for 80 years at the January 2017 Ofsted boarding inspection.

Subject access

The UK GDPR extends to all data subjects and a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests be in place. Where a request for subject access is received from a pupil, the school's policy is that:

- Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.
- The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

Processing subject access requests

Requests for access must be made in writing.

Pupils, parents or staff may ask for a data subject access form, available from the school office. Completed forms should be submitted to the Head of Boarding. Provided that there is sufficient information to process the request, an entry will be made in the subject access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. student record, personnel record), and the planned date of supplying the information (normally not more than 1 month but for complex requests, can be extended for a further 2 months from the request date). Should more information be required to establish the identity of either the data subject (or agent) or the type of data requested, the date of entry in the log would be date on which sufficient information has been provided. Pupils may make requests from age 13.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current education (pupil information) regulations.

Authorised disclosures

The school will in general, only disclose data about individuals with their consent. However, there are circumstances under which the school's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.

- pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
- staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school.

Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who need to know the information in order to do their work. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

A "legal disclosure" is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

An "illegal disclosure" is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.

There will be no disclosure of recorded data to third parties other than authorised personnel such as the Police.

If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However, very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

Requests for images should be made in writing to the Data Protection Officer.

Data and computer security

Lancaster Royal Grammar School undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed).

Physical security

Appropriate building security measures are in place, such as alarms, window bars and deadlocks. Only authorised persons are allowed in the server rooms. Printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are where appropriate, accompanied.

Logical security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly. Data should only be processed on school machines except via an external link to the school network.

Procedural security

In order to be given authorised access to the network, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their data protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are disposed of in confidential waste.

Overall security policy for data is determined by the Headmaster and is monitored and reviewed regularly, especially if a security loophole breach or near-miss becomes apparent. The school's security policy is kept in a safe place at all times.

Any queries or concerns about security of data in the school should in the first instance be referred to the Head of Boarding.

Individual members of staff can be personally liable in law under the terms of the data protection acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

Further details on any aspect of this policy and its implementation can be obtained from the Head of Boarding.

Data Breaches

In the event of a data breach the Data Protection Officer (DPO) will investigate, inform the data subject and the ICO. The DPO will maintain a Data Security

Incident log to record both breaches and potential breaches. Detail of the incident and date are to be recorded as well as action taken as a result.

Record of Processing

The Head of Boarding has carried out a data audit and produced a data map. He keeps this under review.

ACCESS TO PERSONAL DATA REQUEST

Data Protection Act 1998 Section 7.

Enquirer's Surname.....Enquirer's Forenames.....

Enquirer's Address

.....

.....

.....

Enquirer's PostcodeTelephone Number

Are you the person who is the subject of the records you are enquiring about?

YES / NO (i.e. the "Data Subject")?

If NO, do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about? YES / NO

If YES, name of child or children about whose personal data records you are enquiring

.....

.....

.....

.....

Description of Concern / Area of Concern

Description of Information or Topic(s) Requested (In your own words)

Additional information.

Please despatch Reply to: *(if different from enquirer's details as stated on this form)*

Name

Address

Postcode

Data subject declaration

I request that Lancaster Royal Grammar School search its records based on the information supplied above under section 7 (1) of the data protection act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the school.

I agree that the reply period will commence when I have supplied sufficient information to enable the school to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the despatch name and address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent)

Name of "Data Subject" (or Subject's Parent) (PRINTED).....

Dated

LANCASTER ROYAL GRAMMAR SCHOOL CONFIDENTIALITY AGREEMENT

It is the policy of Lancaster Royal Grammar School to provide our employees and pupils with a level of privacy and confidentiality with any information concerning any of our employees or pupils.

In the course of your work, you may have access to confidential information (oral, written or computer generated not otherwise available to the public at large) about employees or pupils, their families and/or personal business. School business information includes computer programs, software and supporting documentation, technological improvement plans, strategic plans, financial information and employee information (including but not limited to co-workers and their families).

THEREFORE, I AGREE that:

My right to enter or make use of confidential information is restricted to my need to know the data or information to perform my job responsibilities. I will keep my computer access password(s) confidential. If another method of accessing a computer system is used, I will restrict its use to myself. I will not discuss any confidential information in any public areas, hallways, gathering spaces etc.

I will hold all confidential information of which I have knowledge in the truest confidence, as required by law. I agree to utilise confidential information obtained by me only for the benefit of the employee or pupil or in performance of my job responsibilities.

Unauthorised disclosure, copying and/or misuse of confidential information is a serious breach of duty and will result in disciplinary action up to and including termination of employment or contract with Lancaster Royal Grammar School. Further, this agreement mandates compliance extending beyond employment contract, or association with Lancaster Royal Grammar School as required by law.

I HAVE READ THIS CONFIDENTIALITY AGREEMENT AND AGREE TO ITS TERMS.

Employee Signature _____

Employee Name (print) _____

Date _____

Annex A ; CCTV

1 PURPOSE

The Purpose of this Annexe to the data protection policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television)

CCTV systems are installed in premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day.

CCTV surveillance at the school is intended for the purposes of:

- protecting the school buildings and school assets, both during and after school hours;
- promoting the health and safety of staff, pupils and visitors as well as for monitoring student behaviour;
- preventing bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- ensuring that the school rules are respected so that the school can be properly managed.

The system does not have sound recording capability.

The CCTV system is owned and operated by the school, the deployment of which is determined by the school's leadership team.

The school's CCTV is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2016/679.

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are made aware of their responsibilities in following the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of recorded images.

2. SCOPE

This Annex to the data protection policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. The school complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its use.

CCTV warning signs will be clearly and prominently placed at the main external entrance to the school. Signs will contain details of the purpose for using CCTV.

In areas where CCTV is used, the school will ensure that there are prominent signs placed within the controlled area. The planning and design have endeavoured to ensure that the system will give maximum effectiveness and efficiency, but it is not guaranteed that the system will cover or detect every single incident taking place in the areas of coverage.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies and related legislation. Video monitoring of public areas for security purposes within school premises is limited to uses that do not violate the individual's reasonable expectation to privacy. Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of the school or a student attending the school. All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by the school.

CCTV monitoring will never be used in any observing or monitoring a member of staff's performance.

3. LOCATION OF CAMERAS

The cameras are sited so that they only capture images relevant to the purposes for which they have been installed (as described above), and care will be taken to ensure that reasonable privacy expectations are not violated. The school will ensure that the location of equipment is carefully considered to ensure that the images captured comply with the legislation. The school will make every effort to position the cameras so that their coverage is restricted to the school premises, which includes both indoor and outdoor areas.

CCTV will NOT be used in classrooms but in limited areas within the school that have been identified by staff and pupils as not being easily monitored.

Members of staff will have access to details of where CCTV cameras are situated. CCTV Video Monitoring and Recording of Public Areas may include the following:

- a. Protection of school buildings and property: The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services
- b. Monitoring of Access Control Systems: Monitor and record restricted access areas at entrances to buildings and other areas
- c. Verification of Security Alarms: Intrusion alarms, exit door controls, external alarms
- d. Video Patrol of Public Areas: Parking areas, Main entrance/exit gates, Traffic Control
- e. Criminal Investigations (carried out by the police): Robbery, burglary and theft surveillance.

4.ACCESS TO CCTV IMAGES

Access to recorded images will be restricted to the staff authorised to view them and will not be made widely available. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher. The Headteacher may delegate the administration of the CCTV System to another staff member. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

5.RESPONSIBILITIES

The Headteacher will:

- a. Ensure that the use of CCTV systems is implemented in accordance with this policy.
- b. Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within the school.
- c. Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy.
- d. Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy.
- e. Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system.
- f. Ensure that monitoring recorded tapes are not duplicated for release.
- g. Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally.
- h. Give consideration to both students and staff feedback/complaints

regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.

- i. Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place.
- j. Ensure that external cameras are non-intrusive in terms of their positions and views of neighboring residential housing and comply with the principle of “Reasonable Expectation of Privacy”.
- k. Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only.
- l. Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 31 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil).
- m. Ensure that camera control is solely to monitor suspicious behavior, criminal damage etc. and not to monitor individual characteristics.
- n. Ensure that camera control is not infringing an individual’s reasonable expectation of privacy in public areas.

6. DATA PROTECTION IMPACT ASSESSMENTS AND PRIVACY

CCTV has the potential to be privacy intrusive. The school will perform a Data Protection Impact Assessment when installing or moving CCTV cameras to consider the privacy issues involved with using new surveillance systems to ensure that the use is necessary and proportionate and address a pressing need identified.

7. POLICY REVIEW

The Data Protection Officer is responsible for monitoring and reviewing this policy. This policy will be reviewed annually. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.