LANCASTER ROYAL GRAMMAR SCHOOL

POLICY STATEMENT

Number	Date Approved By Governing Body
56	July 2018

DATA PROTECTION POLICY

The Governing Body 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 Governors 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. At the time of writing the Data Protection Bill 2017 is progressing through Parliament and will be the basis of a new Act which encompassed the EU's GDPR (General Data Protection Regulations). The GDPR come into force from 25th May 2018. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities ~~within~~ by these guidelines.

Guiding Principles – *GDPR*

The following is a summary of *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 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 is an example of data.

"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 registration 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 assistant headmaster ICT and systems who the person is 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 Governing Body 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 Assistant Headmaster ICT and systems 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 Assistant Headmaster ICT and systems 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 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 is 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.

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 Assistant Headmaster ICT and systems. 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 either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will 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.

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 room. 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 shredded before disposal.
Overall security policy for data is determined by the Headmaster and is monitored and reviewed regularly, especially if a security loophole or breach 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 Assistant Headmaster ICT and systems.
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 assistant headmaster ICT and systems.

Data Beaches

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 Assistant Headmaster ICT and Systems has carried out a data audit and produced a data map. He will keep 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 Postcode ……Telephone 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 and etc.
I will hold all confidential information of which I have knowledge in the truest confidence, as required by law. I agree to utilize 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 _____