Lord Grey Academy

DATA PROTECTION & GDPR POLICY

June 2019

Mission Statement

'Lord Grey Academy is a future-driven, aspirational and inclusive academy offering all learners outstanding social and academic opportunities. Our international, national and local community links promote the development of fulfilled and successful young people. We aim to maximise learner potential to the highest academic levels and to encourage a love of learning that will last a lifetime. We are a high achieving academy with an ambition to become an outstanding first choice local academy '.

Motto: Aspire, Learn, Achieve

POLICY MANAGER:	**Debbie Hawkins**
COMMITTEE:	**Resources Committee**
REVIEW DATE:	**Summer 2019**
NEXT REVIEW DATE:	**Summer 2020**

TABLE OF CONTENTS

1. General and Background

The Data Protection Act 1998 is the law that protected personal privacy and upheld individual's rights. It applied to anyone who handled or had access to people's personal data.

The General Data Protection Regulation (GDPR) over-rides the 1998 Act and is applicable for schools from May 2018. It will apply to all those who process personal data from 25 May 2018 and will replace the previous Data Protection Act.

The board of trustees, delegated to the local governing body, as the body with corporate responsibility for managing the school, has ultimate responsibility for matters relating to data protection. Governors and trustees have a duty to ensure that their school is compliant.

The GDPR imposes new requirements (relating to the appointment of a data protection officer (DPO) and notification of personal data breaches) and provides new rights for individuals. All schools will be subject to the requirements of the GDPR.

The main changes are:

While the general concepts and principles under the 1998 Data Protection Act will remain the same, a number of enhanced definitions and new obligations will increase an individual's rights and possible sanctions.

Under the GDPR, the definition of personal data will include identification numbers, online identifiers and/or location data as well as factors relating to the physical, psychological, genetic, mental, economic, cultural or social identity of a natural person. Accordingly, from May 2018 data such as an IP address or roll number will also amount to personal data.

Sensitive personal data will be replaced by special categories of personal data, which again will extend coverage to include "the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person". "Explicit" consent will usually be required when processing data within the various special categories (unless one of the grounds for processing such data has been satisfied).

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the new Data Protection Act. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

2. Scope of the Policy

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The school collects a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection, as well as the many different types of research data used by the school. In addition, it may be required by law to collect and use certain types of information to comply

with statutory obligations of Local Authorities (LAs), government agencies and other bodies, such as student destinations data.

Lord Grey Academy is committed to the protection of all personal and sensitive data for which it holds inline with the new requirements of GDPR 2018. All aspects of data protection outlined in the GDPR will be covered by this policy and the overarching ethos of this policy will be guided by eight principles.

3. The Eight Principles

The General Data Protection Regulation (GDPR) is based on eight data protection principles, or rules for 'good information handling'.

1. Data must be processed fairly and lawfully and in a transparent manner.
2. Personal data shall be obtained only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed. It will be limited to what is necessary.
4. Personal data shall be accurate and where necessary kept up to date. Where inaccurate data is spotted it should be erased or rectified without delay.
5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.
6. Personal data shall be processed in a secure way.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to another country, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Responsibilities

The school must:

- manage and process personal data properly
- protect the individuals' right to privacy
- provide an individual with access to all personal data held on them.

The school has a legal responsibility to comply with the GDPR. The school, as a corporate body, is named as the Data Controller under the GPDR.

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the GDPR.

The school is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website at the following link :
www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

Every member of staff that holds personal information has to comply with the GDPR when managing that information.

The school is committed to maintaining the eight principles at all times. This means that the school will:

- inform 'Data Subjects' why the school needs their personal information, how they will use it and with whom it may be shared, this is known as a Privacy Notice
- check the quality and accuracy of the information held
- apply sensible records management protocols and procedures to ensure that information is not held longer than is necessary
- ensure that when information is authorised for disposal it is done appropriately
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- only share personal information with others when it is necessary and legally appropriate to do so
- set out clear procedures for responding to requests for access to personal information known as 'subject access'
- train all staff so that they are aware of their responsibilities and of Lord Grey's relevant policies and procedures.

This policy will be updated as necessary to reflect best practice or amendments made to the General Data Protection Regulation.

5. Key personnel

As part of Tove Learning Trust, the school's compliance with GDPR will be guided by a number of key post holders:

- the Multi Academy Trust's (MAT) Chief Executive Officer (CEO) and Chair of the Board of Trustees will ensure that there is a Data Protection Officer (DPO) in place for the MAT
- the overall DPO for Tove Learning Trust is the trust's Director of Business. Who takes advice from Browne Jacobson and EPM and other sources (The Key, NGA etc) on data compliance good practise. They will liaise with the Information Commissioner's office (ICO) and MAT CEO if there are any breaches
- the local DPO for Lord Grey Academy is the academy's Business Manager. Who will follow the advice from the trust wide DPO and ensure that good practise is evident at school level. They will liaise with the Information Commissioner's office and MAT DPO if there are any breaches.
- the Principal of Lord Grey Academy, along with the Chair of the Local Governing Board, ensure that the school has a good quality policy in place and carry out a termly review, via Resources Committee, that all legal and good practise aspects of GDPR are being adhered to
- the Designated Safeguarding Lead (DSL) will act as a quality assurer at academy level in terms of any data regarding students, to ensure that the academy maintains the highest standards of ethical practise in terms of data protection for students.
- the ICT Network Manager, Data Manager, Finance and Office Manager, Attendance Officer, Registrar, Principal's Personal Assistant and Senior Leadership Team Administrators will liaise on a regular basis with the local DPO to ensure that GDPR are adhered to.

6. Data Security

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Where necessary, risk and impact assessments shall be conducted in accordance with guidance given by the ICO. Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and these organisations shall provide evidence of the competence in the security of shared data.

7. Photographs, Video's and CCTV

Images of staff, parents, visitors and students may be captured on CCTV footage for the use in school and where necessary would be shared with law enforcement.

Images of staff and students may be captured at appropriate times and as part of educational activities for use in school only. Unless prior consent from parents/students/staff has been given, the school shall not utilise such images for publication or communication to external sources.

It is the school's policy that external parties (including parents) may not capture images of staff or students during such activities without prior consent.

8. Data Disposal

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, electronic etc) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services. All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance. The school has identified a qualified source for disposal of IT assets and collections.

9. Subject Access Enquiry

The applicant should make initial contact with the Principal's PA and must satisfy him / her that the person making the request is entitled to access the information being requested.

Once agreed, a request must be submitted in writing accompanied with the required fee requesting a 'Subject Access Enquiry'. A response will be issued within 40 days (or five

months in the case of examination data), by post to the home address. (The form is in Section 8 of this document). These are the statutory timescales.

However, as good practice the school would aim to process such information within 20 working days, where possible.

The response will take the form of a printed copy of all data records relating to the student, together with an explanatory letter. The fee required by the school is up to £10 to cover the cost of administrative effort and photocopying involved in processing each request. If a significant amount of information is being requested an increased fee may be applicable. Cheques should be made payable to Lord Grey Academy. The Freedom of Information Act 2000 allows for a charge for photocopying, etc.

10. Misuse

Misuse or abuse of school information covered by the GDPR will lead to an investigation and possible disciplinary action.

Any concerns about use of data in the school should be passed to the local DPO.

Major infractions will be passed to the MAT DPO and may be referred to the ICO for further investigation.

The ICO has the right to fine a MAT or a school if a major infraction of GDPR has taken place.

Any person can appeal to the Chair of Governors of the Local Governing Body if they feel that the DPO has not given sufficient credence to a concern raised about infraction of GDPR. Beyond this an appeal to the Board of Trustees at Tove Learning Trust MAT level is permissible.

11. Further training and information

The Information Commissioner's Office website is (www.ico.gov.uk) and this provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. The Guide to Data Protection which is available from the ICO website gives guidance too.

The local DPO ensures that a schedule of relevant training, as needed, is available to key staff working in the area of data protection. A GDPR working party, which meets termly, helps to further steer the GDPR work of the academy.

The local DPO will raise awareness in the school and through training of staff about the requirements around data protection; monitor compliance with the GDPR and other legal data protection requirements including related school policies (e.g. Charging and Remissions Policy, Whistleblowing Policy, Careers Policy); ensure that there are related data protection impact assessments (DPIAs) and audits in place.

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact the local DPO and Business Manager at Lord Grey Academy.

12. Changes Log

Change	By whom	When
Created	Tracey Jones	24.05.18

13. Subject Access Form

Subject Access Enquiry
Name of Student:
Name of person requiring data access on the student named above and relationship to that student:
Details of the enquiry/request:
Name (Please print) ……
Signature …….. Date ……..
Return to Director of Business with the appropriate fee. All requests will be considered on an individual basis.