

GDPR Compliance Statement

Introduction

The EU General Data Protection Regulation (“GDPR”) comes into force on 25th May 2018 and brings with it the most significant changes to data protection law in two decades. The new Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information. It applies to all organizations which process or handle personal data.

Loughborough Schools Foundation, the organisation with responsibility for Loughborough Grammar School, Loughborough High School, Fairfield Preparatory School and Loughborough Amherst School, is committed to compliance with all relevant EU and UK laws in respect of personal data, and the protection of the rights and freedoms of individuals whose information we collect and process in accordance with the GDPR. Ongoing compliance is embedded in all processes and policies throughout our organisation.

We’ve outlined the policy, system, and operational changes that have been implemented in the Foundation and individual schools to comply with the GDPR.

How we are preparing for the GDPR

- Information Audit– carrying out an information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.
- Policies & Procedures – revising our data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including:
 - Data Protection Policy – our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.
 - Data Breaches – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.
 - Subject Access Request (SAR) – we have revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail the steps to be taken and who is responsible for responding to any SAR.
 - Legal Basis for Processing – we are reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to.
 - Privacy Notice/Policy – we are revising our Privacy Notice to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are,

who the information is disclosed to and what safeguarding measures are in place to protect their information. We have created specific notices for certain parts of our activities, including the School Shop and the Development Office.

- Processor Agreements – where we use any third-party to process personal information on our behalf (*i.e. Payroll, external teaching resources*) we have ensured that they meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.

Information Security & Technical and Organisational Measures

We take the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including:

- Information Security Policy – we classify our data and apply appropriate technical and organisational controls which are based on this classification. Controls in place include, but are not limited to, a Responsible Use Policy, Staff Conduct Policy and Digital Media Guidance.
- Access Controls – we restrict access to information held in paper format through physical security measures. We also take steps to ensure that information is only shared with those who need it.
- IT security – we have invested in Application Firewalls, Proactive Threat Monitoring & Threat Prevention, Cloud-Based Threat Analysis, Next Generation Anti-Malware and Anti-Ransomware, URL Filtering, Vulnerability Prevention and Intrusion Detection Systems.
- Authentication
- Provision of secure area for sharing documents and information between members of Foundation staff.

We have ensured staff have appropriate training and awareness of the requirements of GDPR and how they apply to their jobs, and will continue to develop this awareness through an ongoing programme of learning and support.

GDPR Roles

We have designated **Ruth Brutnall** as our **Data Protection Officer (DPO)**. She can be contacted via DataProtection@endowedschools.org.