DATA PROTECTION POLICY

EU Rules

The UK has left the EU but continues to abide by EU rules.

EU member states took action to protect personal data through GDPR which came into effect in May 2019. UK put this into law via Data Protection Act.

These rules require UK colleges to update their contracts with organisations outside the EU to include some additional contract clauses.

The UK is currently negotiation its future relationship with the EU and this may lead to further changes in 2021 or later.

Whatever happens on those negotiations, the higher standards set by the UK's Data Protection Act will continue to apply for the foreseeable future. Colleges in the UK remain committed to international exchanges and sharing of good practice. The UK government is drawing up plans for new immigration system which will treat people from non-EU countries on the same basis as EU nationals.

Introduction

This policy will be reviewed as further changes are communicated.

John Leggott College ("the College") needs to keep certain information about its employees, students and other users to allow it to for example monitor performance, achievements, health and safety. It also needs to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must comply with the Data Protection Principles, which are set out in the General Data Protection Regulation 2016 (GDPR).

Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that the data controller (the College) shall be responsible for, and be able to demonstrate, compliance with the principles.

The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed this Data Protection Policy. This Policy outlines what we expect from you in order for the College to comply with its legal obligations and compliance is mandatory.

Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by rules and policies made by the College. Any failure to follow the policy can therefore result in disciplinary proceedings.

The College's Data Protection Officer (DPO) is responsible for overseeing this Policy and, as applicable, developing related policies and privacy guidelines.

Please contact the DPO with any questions about the operation of this Policy or the GDPR, or if you are concerned that this Policy is not being or has not been followed. If the matter is not resolved, it should be raised as a formal grievance.

Data Protection Law

The GDPR and the Data Protection Act 2018 (DPA 2018) have replaced the Data Protection Act 1998 (DPA 1998) as the main legislation governing privacy and data protection matters in the UK. Whilst the GDPR is the main source of data protection law, the DPA 2018 fills in some of the gaps in the GDPR as it relates to the UK. The GDPR and DPA 2018 describes how organisations such as the College must collect, handle and store personal information.

The GDPR applies to **personal data** meaning any information relating to an identified or identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

Equality Statement

This policy applies to all college staff regardless of age, race, disability, religion or belief, gender, sexual orientation, marital or civil partnership status, gender reassignment, pregnancy or maternity, or any other status. All individuals will be treated in a fair and equitable manner recognising any special needs where adjustments can be made. No individual will suffer any form of unlawful discrimination, victimisation, harassment or bullying as a result of this policy.

Data Protection Officer

The College as a corporation is the data controller under the GDPR, and the College Corporation is therefore ultimately responsible for ensuring that implementation.

The College has a designated Data Protection Officer (DPO) (Director of Governance) who is responsible for:

- Maintaining the College's registration with the Information Commissioner's Office;
- Providing advice, guidance, monitoring of compliance and direction regarding data protection matters within the College;
- Reporting personal data breaches where appropriate;
- Raising data protection awareness and providing training to staff regarding data protection law and the GDPR

Data Protection Risks

This policy helps to protect the college from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the college uses data relating to them.
- Reputational damage. For instance, the college could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with the College has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this Policy and the data protection principles.

However, the following have key areas of responsibility:

- The Corporation is ultimately responsible for ensuring that the College meets its legal obligations.

- The DPO is responsible for:
    - Keeping Corporation updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.

- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this Policy.
- Dealing with requests from individuals to see the data that the college holds about them (also called 'subject access requests') and any other data subject rights.
- Checking and approving any contracts or agreements with third parties that may handle the college's sensitive data.
- Reporting data breaches, when required, to the ICO.
- Monitoring compliance and conducting internal audits.

- The IT Manager is responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services the college is considering using to store or process data. For instance, cloud computing services.

- The Principal is responsible for:
  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

- The Director of Finance & Resources is responsible for:
  - Ensuring that Staff data is kept as accurate and up to date as possible.
  - The timely removal/anonymization of data from college systems to abide by the need in GDPR to keep data no longer than is necessary.

- The MIS Manager/Timetabling Officer have shared responsibility for:
  - Ensuring that Student data is kept as accurate and up to date as possible.
  - The timely returns of data to ensure the college fulfils its legal obligations.
  - The timely removal/anonymization of data from college systems to abide by the need in GDPR to keep data no longer than is necessary.
  - Shared responsibility in terms of output, reporting and retention.
  - Consultant in terms of ILR reporting and Senior MIS Officer in terms of personal data collected.

Responsibilities of Staff and Students

All staff and students are responsible for:

- Checking that any information that they provide to the College in connection with their employment or studies is accurate and up to date;
  Informing the College of any changes to or errors in information, which they have provided, i.e. changes of address. They must ensure that changes of address, etc. are notified to Human Resources (staff) and College Information Services (CIS) (students);
  Reporting known or suspected data breaches to the DPO as quickly as possible. The

College cannot be held responsible for any such errors unless the staff member or student has informed the College of them.

Protecting Personal Data

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

These rules describe how and where data should be safely stored and used. Questions about storing data safely can be directed to the IT Manager or DPO.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer, cupboard or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer or photocopier.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data systems can be securely accessed from outside the college using Remote Desktop services. This means personal data should never be removed from site or saved to offsite computers.
- Personal data should be protected by strong passwords that are changed regularly and never shared between employees.
- Personal data should not be stored on removable media (like a CD or DVD). If there is any eventuality where this is required then these should be kept locked away securely when not being used.
- Personal data should only be stored on designated drives and servers, and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Personal data should be backed up frequently. Those backups should be tested regularly, in line with the college's standard backup procedures.
- Personal data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing personal data should be protected by approved security software and a firewall.

Personal data is of no value to the college unless the college can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should not usually be

sent by email, as this form of communication is not secure.
- Only certain designated staff (as designated by the Data Protection Officer) should transfer data offsite. When data is transferred to external agencies then it should be encrypted password protected or use a secure electronic file system.
- Personal data should never be transferred outside of the European Economic Area (without explicit written consent of the individual).
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data Accuracy

The law requires the college to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort the college should put into ensuring its accuracy.

It is the responsibility of all staff who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- The college will seek to make it easy for data subjects to update the information we know about them.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- The College will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the college or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection.

Subject Access Requests

Data subjects have the right to request access to their personal data processed by us. If an individual contacts the college requesting this information, this is called a subject access request (SAR).

Subject access requests from individuals should be made by email, addressed to the data controller at beckyrobinson@leggott.ac.uk.

If personal data of the data subject are being processed, we shall provide the data subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (electronic) means:-

a) The purposes of the processing;
b) The categories of personal data concerned;
c) The recipients or categories of recipient to whom the person data have been or will be disclosed;
d) Where possible, the retention period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing;
f) The right to lodge a complaint with the Information Commissioner's Office (ICO);
g) Where the personal data are not collected from the data subject, any available information as to their source;
h) Whether or not automated decision making is used and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and

We shall also, unless an exemption applies, provide the data subject with a copy of the personal data processed by us in a commonly used electronic form (unless the data subject did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form), within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

If the SAR is manifestly unfounded or excessive, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to act on the request. If we are not going to respond to the SAR, we shall inform the data subject of the reason(s) for not taking action.

The College will always verify the identity of anyone making a subject access request before handing over any information.

Providing Information (Transparency)

The GDPR requires data controllers to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. Such information must be provided through appropriate 'privacy notices' which must be concise, transparent, intelligible, easily accessible, and in clear and plan language so that a data subject can easily understand them.

Whenever we collect personal data directly from data subjects (such as pupils, parents, staff or others) we must provide the data subject with all the information required by the GDPR, including: the identity of the data controller (the College) and the DPO; how and why we will use, process, disclose, protect and retain that personal data, through a privacy notice which must be presented when the data subject first provides the personal data.

When personal data is collected indirectly, you must provide the data subject with all the information required by the GDPR as soon as possible after collecting/receiving the data.

The College aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the college has privacy statements for the following individuals:

- Students
- Student Applicants
- Staff/Workers
- Staff Applicants
- Parents
- Governors
- Host Families
- Letting Users
- Work Experience Providers

These set out how data relating to individuals is used by the College. These are available on request. A version of this statement is also available on the College website.

Personal Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This includes breaches that are the result of both accidental and deliberate causes. If a member of staff or student believes a breach has taken place, they should contact the Data Protection Officer immediately through breach@leggott.ac.uk.

On becoming aware of a data breach a full investigation will be completed by the Data Protection Officer who will contain the situation, assess the potential adverse consequences for individuals, recover the breach if possible and report to the ICO where appropriate within 72 hours. Any individual affected by a significant breach will be informed including the measures taken to mitigate any possible adverse effects.

Any security incident will be investigated to determine if the breach was a result of human error, a system error or of a malicious nature. Further staff training and revisions to systems may take place as identified following the investigation. All staff are aware that any breach of the General Data Regulations Policy may result in the college's disciplinary procedures being instigated.

Periodic Review of Data Protection Policy

The Data Protection Officer should review the Data Protection Policy annually and we reserve the right to change this Data Protection Policy at any time without notice to you.

Policies/Plans to Cross Reference

The Data Protection Officer should review the Data Protection Policy annually and we reserve the right to change this Data Protection Policy at any time without notice to you.

- Data Retention & Erasure Policy
- Records Management Policy
- Procurement Policy
- Strategic Development Plan
- Risk Register

APPENDIX A
Glossary of Terms

Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data controller: is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by the Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data subject: a natural person whose personal data is processed by a data controller or processor.

Personal data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Privacy impact assessment: a process designed to help organisations identify and mitigate privacy risks associated with proposed data processing activities. For further information, see the University's Privacy Impact Assessment guidance.

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pseudonymisation: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Restriction on processing: the marking of stored personal data with the aim of limiting their processing in the future.

Right of access: entitles the data subjects to have access to have access to and information about the personal data being processed by the data controller.

Special categories of personal data: personal data revealing a data subjects racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership or the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Policy Owner:	Becky Robinson	Next Review Date:	June 2023