LONDON CHURCHILL COLLEGE

DATA PROTECTION POLICY

Audience	Policy	Version Number and Month	Next Review Due	External Reference Points:
External	Data Protection Policy	V3-July 2018	Jan-2019	The General Data Protection Regulation (GDPR) (EU) 2016/679 ICO Guide to the General Data Protection Regulation Data Protection Act 2018

AIMS

London Churchill College aims to secure and protect the data of its students, staff, applicants to courses and any other individuals for whom it holds personal data. The College will do this in accord with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

This policy sets out the expectations that all College staff, students, contractors, partnership organisations and partner staff who process or use any personal information on behalf of the College are subject to in order to ensure that the College is compliant with its obligations.

DEFINITIONS

The College:
London Churchill College is referred to throughout this policy as “The College”

The Individual:
Any living individual who is the subject of personal data whether in a personal or business capacity. The Data Protection Act, which is designed to protect individuals and personal data, defines the individual as the ‘data subject’. All Individuals, including those who have left the College or whose application to the College has been unsuccessful, shall be covered by this policy.

Data:
Any personal information which relates to a living individual who can be identified. This includes any expression of opinion about the individual. Examples of personal data include:

- A persons’ name and address
- Data of birth
- Statement of fact
- Any expression or opinion communicated about an individual
- Minutes of meetings, reports
- Emails, file notes, handwritten notes, sticky notes
- CCTV footage if an individual can be identified from the footage
- Employment or education history

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. For example, information about an individual’s:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

POLICY PRINCIPLES

- London Churchill College secures data by ensuring staff remain aware and trained in their roles and responsibilities set out by this policy and through the ongoing monitoring of the Data Protection Policy by the Data Protection Officer.
- Individuals have the right to access, correct and delete data within 30 calendar days of a request.
- The College will provide Individuals with clear information on how their data will be stored and the reasons for its collection.
- In the event of a data breaches, the College will report the breach to the ICO and to individuals whose data is compromised within 72 hours of the breach.
- The College ensures that access to personal data is limited to only those who require it for legitimate purposes.
- The Data Protection Officer is responsible for ensuring that the College does not collect information that is not strictly necessary for the purpose for which it is obtained
- Any breach of the this Policy by a staff member may lead to disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

GROUNDS FOR DATA PROCESSING

All processing of Personal Data shall be completed in a lawful, fair and transparent manner.

Public Task
The College considers itself to be a public authority, in line with the ICO Guide to the General Data Protection Regulation and the processing of student data is required to perform its tasks as set down in UK law.

It is a condition of student enrolment and of staff employment that they agree to the College processing certain personal information as part of its statutory obligations. Additionally, the College may also process some information that is categorised as “special category data”. This information may be required to comply with certain government or funding body regulations.

Consent
The College seeks the consent of the individual whom the data concerns before completing any processing that cannot be considered part of its duty as a public authority. This may include the consent to receive Direct Marketing.

When seeking consent from an Individual, the College will always ensure that it is unambiguous and that it involves a clear affirmative action by the Individual. Requests for consent shall include:

- the name of any third party controllers who will rely on the consent;
- an explanation as to why the College would like the requested data and how it shall be processed.
- Information to the Individual on how to withdraw their consent at any time

Consent shall never be a precondition to enrolment at the College.

INDIVIDUAL RIGHTS

The College will ensure that Individuals are made aware of the rights provided to them by GDPR in relation to the processing of their data, including data processed with their consent and data processed under other legal grounds.

Individuals wishing to exercise any of their rights should do so by submitting a request to the Data Protection Officer. This can be done either verbally or in writing. The College will aim to respond to the request within 30 calendar days.

Data Protection Officer
Email: dpo@londonchurchillcollege.ac.uk

The right to be informed
The College will provide Individuals with clear and concise information about how their data will be processed, the purpose for its collection, who it will be shared with and how long it will be stored for. This information is included in the Privacy Policy, which is available on the College website.

All individuals will be directed to the Privacy Policy at the time when their personal data is collected. The Privacy Policy shall be reviewed at least annually, together with this Data Protection Policy.

The right of access
Individuals have the right to a copy of the personal information the College holds about them. Individuals wishing to exercise this right, should contact in the first instance, the Data Protection Officer. The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 calendar days unless there is a good reason for delay.

The right to rectification
The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.

An individual can make a request for rectification verbally or in writing to the DPO. The College will respond to the request within 30 calendar days.

The right to erasure
Individuals have the right to have personal data erased. The right is not absolute and only applies in certain circumstances.

Individuals wishing to have their data erased can do so verbally or in writing to the DPO. The College will comply within 30 calendar days, provided that the data is not required in order to comply with awarding body, government or funding body regulations.

The right to restrict processing
Individuals have the right to request that the College restrict the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their personal data and the College is in the process of verifying the accuracy of the data;
- the data has been unlawfully processed and the individual opposes erasure and requests restriction instead;
- the College no longer needs the personal data, but the individual needs the College to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to the College processing their data and the College is considering whether it has legitimate grounds that override those of the individual.

Individuals wishing to restrict processing can do so verbally or in writing to the DPO. The College will comply within 30 calendar days, provided that the data is not required in order to comply with awarding body, government or funding body regulations.

The right to data portability
The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller. The right only applies to data that the College is processing with the Individual's consent, but does not apply to data that the College processes as a public authority.

The right to object
The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. This includes an absolute right to stop their data being used for direct marketing.

An individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their particular situation. In these circumstances the College may continue processing if there are compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

If the College determines that it has grounds to continue processing, then it shall inform the Individual of their right to submit a complaint to the ICO.

PROCESSING AND STORAGE OF PERSONAL DATA

CCTV
CCTV images that show a recognisable person are considered personal data and are therefore covered by this Data Protection Policy.

Individuals have the right to access CCTV images of themselves. Requests to access or to obtain a copy of any CCTV footage should be made in writing to the Data Protection Officer. Individuals will be required to provide Proof of Identification before they will be permitted to access the footage.

The College will provide access to CCTV footage to Third Parties if the requestor satisfies the following criteria

- Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry)
- Prosecution Agencies and their Legal Representatives
- Insurance Companies and their Legal Representatives

By supplying the footage, the College must not disclose any personal data of another Individual. This may involve blurring parts of the footage.

Recorded images will be retained for no longer than 21 days from the date of recording, unless required for evidential purposes or the investigation of crime or otherwise required.

Bring Your Own Device (BYOD)
Staff wishing to use their own device for College work must ensure that any personal data of the College that is stored on their device is appropriately protected. This includes visitors (such as external examiners or reviewers) who might receive access to personal data. If necessary, staff should seek help from the IT department meet the BYOD requirements set out in this policy:

- Set and use a passcode (e.g. pin number or password) to access your device. Whenever possible, use a strong passcode. Do not share the passcode with anyone.
- Set your device to lock automatically when the device is inactive for more than a few minutes.
- Take appropriate physical security measures. Do not leave your device unattended.
- If other members of your household use your device, ensure they cannot access College information, for example, with an additional account passcode. (Our preference is for you not to share the device with others.)
- Organise and regularly review the information on your device. Delete copies from your device when no longer needed
- When you stop using your device (for example because you have replaced it) and when you leave the College's employment, securely delete all (non-published) College information from your device.
- Encrypt the device (to prevent access even if someone extracts the storage chips or disks and houses them in another device)

If any staff member loses their device or believes the personal data contained on their device may have been breached, they must report this immediately to the DPO.

Data Retention Period
The College is not permitted to keep personal information of either applicants, students or staff for longer than is required for its purpose. However, some data will be kept longer or in perpetuity to comply with statutory or funding body requirements. Personal and confidential information will be disposed of by means that protect the rights of those individuals.

When data held in accordance with this policy is destroyed, it must be destroyed securely in accordance with best practice at the time of destruction.

Data Breaches
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. This includes breaches that are the result of both accidental and deliberate causes.

The College shall report to ICO any potential data breach within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to adversely affect individuals' rights and freedoms, the individuals concerned shall be informed without undue delay.

COMPLAINTS

Individuals wishing to make a complaint with regard to the security of their data, the use of their data or any other data related issue, should do so by contacting the DPO in the first instance.

Data Protection Officer
Email: dpo@londonchurchillcollege.ac.uk
Telephone: +44 (0) 2073771077

However, if the individual remains dissatisfied with the College's response or if they would like to seek advice, they can refer the matter to the Information Commissioner's Office (ICO).

ICO helpline - Telephone: 0303 123 1113
https://ico.org.uk/concerns/

It is also possible to chat online with an advisor: https://ico.org.uk/global/contact-us/live-chat/

TRAINING

The College arranges training for its staff to ensure awareness of this policy and the roles and responsibilities it sets out to staff.

Workshops with Brand Advocates are held during each admission intake to provide Brand Advocates with information about courses. These are also used as a refresher session for the Terms and Conditions of the Brand Advocate agreement, which include Data Protection.

MONITORING

The DPO is responsible for monitoring the implementation of this policy and will report to the Principal's Executive Group if the policy is not being followed or to bid for further resources.

Department heads are responsible for ensuring that their staff abide by the Data Protection Policy and must report to the DPO if any potential Data Breach has occurred.