THE FACULTY OFFICE

Data Security Policy
(May 2018)

Policy statement

This new policy is issued following the introduction of the EU General Data Protection Regulation 2015 which came into force on 28 May 2018.

The principles set out in the GDPR are set out in the Annex.

Data under this policy is defined as "any information related to a natural person or data subject that can be used to directly or indirectly identify that person."

This policy sets out the practice of the Faculty Office on Data handling and its security.

The Faculty Office aims to protect Data from all threats (deliberate or accidental) whether internal or external. It aims to ensure a proper awareness and understanding of the need for Data security.

Scope

- The Faculty Office issues three types of faculties and this policy covers Data is held for all three functions:
    - **Special Marriage Licences** – for couples to marry in a particular church building where they could not otherwise obtain the correct legal permission.
    - **Notarial faculties** – to appoint a person as a Notary and to permit them to practise.

    - **Lambeth degrees** – to award a full degree to a person who has not been awarded that degree by another academic institution.

- The policy extends to data held on Notaries practicing within non EU jurisdictions:
    - **Jersey and Guernsey**
    - **Gibraltar**
    - **New Zealand and Queensland (Australia)**
    - **Papua New Guinea**

- The policy also extends to data held on employees of and contractors to the Faculty Office.

Consent

By providing Data, applicants for special marriage licences, notaries (and all persons applying to be admitted as notaries) and recipients of Lambeth degrees consent to its use by the Faculty Office.

Persons submitting any Data in connection with any form of complaint against a notary also consent to its use by the Faculty Office.

The Faculty Office will state, where it considers appropriate, where/how that Data will be used.

Data security

For the purpose of this policy Data security covers:

- confidentiality (prevention of the unauthorised disclosure of information),
- integrity (prevention of the unauthorised amendment or deletion of information);
- security (the prevention of unauthorised access to information).

Application of this Policy

This policy applies to all third parties with whom the Faculty Office shares Data. This includes employees and contractors.

This policy expressly extends to those employees of Lee Bolton Monier-Williams (LBMW) who have responsibility for retention, management and maintenance of Data on behalf of the Faculty Office.

Expectations of employees

All employees of the Faculty Office (and the relevant employees of LBMW) are required to:

- Be mindful at all times of their obligations to respect privacy and confidentiality.
- Head communications "private and confidential" as appropriate.
- Ensure their computer/laptop on which any Faculty Office Data is stored is password protected, and that the password is kept confidential.
- Keep up to date suitable virus protection on their computer/laptop.
- Refrain from the use of memory sticks and discs for data storage
- Exercise care when taking phone calls to avoid any breach of confidentiality.
- Double check the recipients of their emails before sending.
- Refrain from opening any email or attachment which looks suspicious.
- Return all documents, data and equipment on which Data is stored on request of the Faculty Office or when leaving the employment by the Faculty Office.
- Continue to respect confidentiality (unless expressly released) after their contractual arrangement with the Faculty Office has concluded.

Data retention

The Faculty Office will only retain Data where it has a legitimate basis to do so including (but not limited to the powers granted under:

- The Ecclesiastical Act 1533 (Special Marriage Licenses)
- Education Act 1988 (Lambeth Degrees)
- The Courts & Legal Services Act 1990 and under the Legal Services Act 2007 (Notaries);

And also in compliance with other public laws.

Whilst the Faculty Office will keep the period for which Data is retained under review (and Data will be kept for a minimum of 6 years), the Faculty Office consider that its statutory obligations require Data generally to be kept indefinitely to ensure evidence can be provided of due process.

Access to Data

The Faculty Office will limit access to Data to those who require it to:

- Undertake the three roles of the Faculty Office described above
- Otherwise undertake the statutory and regulatory functions of the Faculty Office e.g. the Legal Services Board, the Legal Ombudsman, and other approved regulators.
- Fulfil the legal obligations of the Faculty Office e.g. to the courts and the Police.

AND

- Undertake services for the Faculty Office including but not limited to:

    - membership of the Faculty Office Advisory Board and Qualifications Board
    - IT development and maintenance including the website
    - marketing and events management

Publication of disciplinary outcomes

The control of this published information is covered under the Faculty Office policy on Publication of Disciplinary outcomes.

Control: Data audit

The Faulty Office maintains a record identifying, inter alia:

- What Data is being held.
- To whom the Data relates.
- Where the Data came from.
- The frequency of collection of that Data.
- In what form the Data is held e.g. electronic or hard copy.
- The right of the Faculty Office to collect that Data.
- With whom the Faculty Office shares that Data.

This record is kept under review on an ongoing basis.

Control: Data control system

The Faculty Office documents the controls it exercises in relation to:

- General Data.
- Data held electronically.
- Data held manually.

Controls are kept under review on an ongoing basis (and will be formally reviewed every two years).

Data protection registration

The Faculty Office will at all times maintain a current and relevant data protection registration with the Information Commission Officer. All parties captured by this policy will respect the terms of that registration, seeking clarification on a needs be basis from the Chief Clerk of the Faculty Office to avoid any breach.

Access to Data

The Faculty Office will respond within 1 calendar month (which may be extended by the Faculty Office by a further two calendar months if the requests are numerous or complex) to any request for access to and/or confirmation of Data being processed by the Faculty Office, by an individual to whom that Data relates. The Faculty Office will charge the applicable statuary fee (if any) for this information unless it considers the request to be manifestly unfounded or excessive, particularly if it is repetitive, in which case a reasonable fee (based on administrative costs) will be charged.

In the event the Faculty Office refusing an access request, it will explain in writing its reasons for doing so, advising of the right to refer the matter to the ICO.

Objection to Data processing

The Faculty Office will comply with a legitimate objection to processing Data unless it can demonstrate compelling legitimate grounds for doing so, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise and defence of legal claims.

Data correction and Data erasure

Upon receiving a valid request the Faculty Office will:

- correct incorrect Data;
- (but having due regard to the statutory and regulatory duties of the Faculty Office and the public interest in the availability of the data in question) delete Data. The Faculty Office will then also require third parties with whom it has shared Data to erase that Data. If the Faculty Office refuses a request for the deletion of Data it will give its reasons.

Data Destruction

In view of the significance of the Data held (such as evidence of a special licence to marry and the information provided to grant that licence) Data will generally be retained indefinitely but the Faculty Office reserves the right to erase Data (and in particular to destroy files and other hard copy material) where (in its absolute discretion) that Data is deemed obsolete by the Faculty Office.

Data Protection officer

Having regard to the nature of the operation of the Faculty Office and the management of Data for the Faculty Office by LBMW there will be no appointment of a data protection officer for the Faculty Office. The Chief Clerk of the Faculty Office (in close liaison with the Data Protection Officer of LBMW) will monitor data management.

Data impact assessment

Based on the Faculty Office Data processing activities, it is not considered appropriate to undertake a Data protection impact assessment.

Breach of policy

Any breach of this policy, actual or suspected, must be reported immediately or as soon as reasonably practicable to the Chief Clerk of the Faculty Office by anyone to whom this policy applies. Any breach of this policy by the Chief Clerk of the Faculty Office must be reported by them to the Master of the Faculty Office immediately or as soon as reasonably practicable. A breach by an employee of the Faculty Office may be treated as a disciplinary offence. A breach by a third party e.g. contractor may result in their contract being terminated with immediate effect.

In the event of a breach likely to result in a risk to the rights and freedoms of individuals, the Faculty Office will notify the ICO within 72 hours of the event happening, and affected individuals as required under prevailing data protection legislation.

Review

The Faculty Offices will review this policy periodically and at least one in every four years to ensure it remains current and fit for purpose.

Appendix

The EU General Data Protection Regulation (GDPR) – summary

- The EU General Data Protection Regulation (GDPR) came into force on 25 May 2018. It replaces all data protection legislation in EU member states.

- The data protection principles state that personal data must be:
    - Processed fairly, lawfully and in a transparent manner.
    - Collected for specified explicit and legitimate proposes.
    - Adequate, relevant and limited to what is necessary.
    - Accurate and up to date.
    - Kept in a form that permits identification of the data subjects for no longer than is necessary.
    - Processed with appropriate security.

- The rights of the data subject are:
    - Access
    - Rectification
    - Object to direct marketing
    - Processed only for restricted purposes
    - To call for data to be transferred
    - Erasure