

## ST CATHERINE'S COLLEGE

## THE GENERAL DATA PROTECTION REGULATION

### Requirements

The General Data Protection Regulation (GDPR) comes into effect on 25 May 2018. Under Article 5 of the GDPR, the 6 principles relating to the processing of personal data are defined. Data must be:-

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to the purposes set for collection
4. Accurate and kept up to date
5. Retained for no longer than for the purposes set for collection
6. Held securely

### Implementation Activities

In order to fulfil these conditions, St Catherine's College, working together with the University of Oxford, Conference of Colleges Information Security Group and solicitors employed by the Estates Bursars' Committee - Mills and Reeves - has:

- Contributed to a review of information assets in order to identify classes of information and in relation to each class, establish the grounds for the retention of information (1, 2 and 3 above), privacy notices making clear to those whose data we hold why we hold it, procedures for ensuring accuracy (4 above) and retention arrangements (5)
- Undertaken an assessment of the adequacy of the management and technical aspects of the security of its systems resulting in decisions on the technical and physical characteristics of data processing and policies on management on data security (6 above). A further review of progress made since the first maturity assessment in 2017 is anticipated shortly.

## [Future Compliance](#)

In advance of 25 May the College will have completed the work needed to provide a framework for fulfilment of the requirements of the GDPR.

Thereafter, the College will need to make sure that those processing information on its behalf are complying with this framework. In order to do this your attention is drawn to the following links:

- 1 The [College Information Security Policy](#) approved by Governing Body in November 2014. This has been revised to take account of the requirements of GDPR and will return to Governing Body in Trinity Term 2018 for a further review.
- 2 The [Information Security website of the University of Oxford](#). The College has decided that, rather than generating further guidance, it wishes to rely on that provided by this University site.

Where reference is made in the University's Information Security website to the University Information Security Policy you are to refer to the [College Information Security Policy](#).

Where the University site refers to bodies or roles which do exist within the College (for example, Divisions and Heads of Division), the responsibilities attached to such University bodies or roles are as defined for College bodies and roles in the [College Information Security Policy](#).

In particular, technical assistance is available in the College from the College IT Manager. Breaches of data security should be reported, in the first instance to the IT Manager and Home Bursar.

- 3 All those employed by the College are required to complete the [Information Security Awareness Module](#) on appointment and annually thereafter. A copy of the record of completion of the module is to be sent to the Human Resources Advisor who will ensure that the record is held on file.