ST PETER’S
COLLEGE
UNIVERSITY OF OXFORD

Information Security – Good Safe Practice

The terms of the GDPR make incumbent upon all those with access to sensitive personal data the duty of keeping such data secure, and releasing personal information only with the express permission of the individual to whom it relates. Breaches of the legislation can trigger large fines, and cause distress and anger to those whom they affect.

This makes it imperative that all members of College dealing with such data should take steps to protect data, which include, but are not necessarily limited to, the following:

- Preserving the security of such data in a physical sense by keeping sensitive or confidential documentation under lock and key, and by ensuring that networked devices (including tablets, smartphones, etc.) are kept secure and password- or PIN protected, and by using the recommended arrangements for the disposal of confidential waste

- Where required, encrypting sensitive or confidential data (e.g. when placed on portable devices such as flash drives)

- Keeping anti-virus, firewall, and operating system software up to date and patched at all times, and making sure it is of the best available standard

- Not opening any suspicious emails or attachments, which may contain spyware and malware; such emails must be forwarded to JICTS.

- Taking extreme care when, for example, sending out mass mailings, and using the ‘reply to all senders’ facility in email

- Logging out of sensitive sites (e.g. OxCort, admissions databases such as ADSS, Nexus 365, registration) when they are not in use

- Exercising especial care when working outside College and University workspace, and particularly when using free wireless systems

- Always reading carefully, and acting upon, advice relating to security sent by JICTS (and, where relevant also, Faculty) staff

- Where sensitive or confidential information is concerned, do not use commercial file-sharing sites such as DropBox, WeTransfer, and commercial 'cloud' services

- Considering carefully whether information would be better communicated non-electronically: by a face-to-face meeting, in MS Teams, telephone conversation, or on paper (sent registered if committed to the ordinary post).

All members and employees of St Peter’s College should take care to read and understand the information relating to information security. They undertake to observe safe practice when they have access to sensitive personal data.