Nuffield College
UNIVERSITY OF OXFORD

Nuffield College Information Security Policy

2017

The following policy has been approved by Governing Body and its Information Systems Committee. Any amendments to the policy require Governing Body's approval. Each member of the College, and any user of College systems or network, is required to comply with this policy. Support and guidance for departments is offered by Nuffield College's IT Team which in turn is supported by the University's central Information Security Team. Information Security is not a new requirement, and to a large extent the policy and accompanying procedures formalise and regularise existing good practice within the College and wider university.

Nuffield College Information Systems Committee is required by its Governing Body to review this policy yearly to ensure any new developments are covered and protected.

Title	Nuffield College Information Security Policy		
		Document status	Approved

Owner	Director of IT/Bursar
Approver(s)	Governing Body

Version	Version history	Version date
1.0	Approved by GB 29 November 2017	Michaelmas 2017

Nuffield College
UNIVERSITY OF OXFORD

Nuffield College Information Security Policy

1 Purpose

This policy outlines Nuffield College's approach to information security management and sets out the fundamental principles and responsibilities which ensure Nuffield College's security objectives are met.

2 Definitions[1]

Personal data is commonly defined as data which relate to a living individual who can be identified from that information, or from that and other information which is in the possession of, or is likely to come into the possession of, the College.

Sensitive personal data includes information relating to race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life or criminal activities.

Confidential data is a more generalised term, which in some contexts may be used to include personal or sensitive personal data. In the context of this policy, it pertains to data that could cause embarrassment, reputational damage, or liability to legal action for individuals or for the College in general.

3 Scope

The College has legal responsibility[2] for its use of personal data. Everyone has to follow strict rules called 'data protection principles'. They must make sure any personal data is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

There is stronger legal protection for **sensitive personal data** within the Data Protection Act, 1998 (DPA1998).

Note that personal data, already in the public domain (e.g. collections of references) are excluded from the scope of the DPA1998, and therefore similarly outside of the scope of this policy.

This policy is applicable across Nuffield College, its members, visitors and any users of its systems and networks, and applies to:

- all individuals who have access to Nuffield College information and technologies;
- all facilities, technologies and services that are used to process College/University information;

[1] See https://www.admin.ox.ac.uk/councilsec/compliance/dataprotection/definitions/ for more specific definitions.

[2] See https://www.gov.uk/data-protection/the-data-protection-act (DPA 1998) and http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG (GDPR)

- information processed, in any format, by Nuffield College pursuant to its operational activities;
- internal and external processes used to process College/University information; and
- external parties that provide information processing services to Nuffield College.

4 Objectives

Nuffield College's objectives for information security are that:

- information security is considered within all teaching, research and administration activities;
- individuals are aware and kept informed of their information security responsibilities;
- information security responsibilities are clearly identified and communicated to committees and members of College through job descriptions, terms of reference and other appropriate means;
- information risks are identified, managed and mitigated to an acceptable level;
- authorised users can securely and straightforwardly access information to perform their roles;
- facilities, technologies and services adequately balance usability and security;
- implemented security controls are pragmatic, effective and measurable;
- contractual, regulatory and legal obligations relating to information security are met; and
- incidents are effectively managed and resolved, and learnt from to improve our control environment.

5 Information Security Policy Framework (ISPF)

Information is critical to Nuffield College's operations and failure to protect information increases the risk of financial and reputational losses. The College is committed to protecting information, in all its forms, from loss of **confidentiality**, **integrity** and **availability** ensuring that:

- all who handle confidential or sensitive data, complete information security awareness training;
- information security risk is adequately managed and risk assessments on IT systems and business processes are performed where appropriate;
- all relevant information security requirements of the College are covered in agreements with any third-party partners or suppliers, and compliance against these is monitored;
- appropriate information security controls are implemented to protect all IT facilities, technologies and services used to access, process and store College information;
- all information security incidents are reported in a timely manner via appropriate management channels, information systems are isolated, and incidents properly investigated and managed;
- Information Asset Owners are identified for all College information assets[3], assets are classified according to how critical and sensitive they are, and rules for their use are in place; and
- information security controls are monitored to ensure they are adequate and effective.

To provide the foundation of a pragmatic information security framework, Nuffield College uses a set of minimum information security controls, known as the baseline, either as published by the University's Information Security team or of equivalent strength. Where research, regulatory or

[3] An information asset represents a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Examples include databases, booking systems, web sites with log-in accounts etc.

national requirements exceed this baseline, controls will be increased at necessary service or project level. Where it is not possible or practicable to meet the baseline, exceptions will be documented to justify the deviation and appropriate compensating controls will be put in place. The baseline assessment supports the College in achieving its information security objectives.

The policy and the baseline shall be communicated to users and relevant external parties, and linked to from the College website.

6 Responsibilities

The following bodies and individuals have specific information security responsibilities:

- **The Bursar**, in conjunction with the Director of IT, is accountable for the effective implementation of this information security policy, and supporting information security rules and standards.
- **Governing Body**, informed by the **Information Systems Committee** (ISC), has responsibility for overseeing information security within College and for ensuring compliance. ISC is responsible for identifying and managing security risks to the College's staff and students, its infrastructure and its information.
- **The Bursar** is responsible for establishing and maintaining the College's information security management framework to ensure the availability, integrity and confidentiality of the College's information. The Bursar, with the support of the Director of IT, will lead on the definition and implementation of the College's information security arrangements.
- **All employees and members of College** are responsible for making informed decisions to protect the information that they process and for complying with all relevant policies and procedures.
- **Suppliers to the College** are expected to take appropriate steps to comply with this policy commensurate with the nature of the service being provided.

7 Compliance

Nuffield College shall conduct information security compliance and assurance activities, facilitated by the University's Information Security Team, to ensure information security objectives and the requirements of the ISPF are met. Wilful failure to comply with the policy and baseline may result in enforcement or disciplinary action on a group and/or an individual. This policy is informed by the 1998 Data Protection Act and the European Union General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

8 Review and Development

This policy, and supporting information security documentation, shall be reviewed and updated by the Bursar, the Director of IT and approved by Information Systems Committee on an annual basis to ensure that they:

- remain operationally fit for purpose;
- are proportionate to the identified risks;
- reflect changes in technologies;
- are aligned to industry best practice; and
- support continued regulatory, contractual and legal compliance.

9 Nuffield College information security rules and guidance

Users of ICT within the University are subject in the first instance to the **University ICTC regulations (2002)**[4].

Nuffield College has its own set of Information, Data and Network security rules which must be followed by members of College, particularly when handling personal data. These rules can be found at:

- https://www.nuffield.ox.ac.uk/go/it-rules (Network rules)
- https://www.nuffield.ox.ac.uk/go/infosec-guidelines (Information Security detailed rules and guidelines)

All members of College must read the above guidelines before using College systems.

[4] http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml