St Stephen's House
Information Security & Data Protection Policy

Title	Information Security Policy 09_2017
Date of Drafting	31 August 2017

Document owner	IT Manager
Approver	Data Controller, Bursar, Principal

Version	Version History	Version Date
0.1	Initial Draft from University Template	15 August 2017
1.0	Approval by House Council	9 September 2017
1.1	Update of Data Protection Policy re. GDPR	10 May 2018

Preface and document control

This document is intended to provide information security policy, procedure, standards or guidance in respect of St Stephen's House and shall be reviewed at least annually to ensure validity.

Part I – Approach to Information Security

1. Purpose

This policy outlines St Stephen's House's approach to information security management and provides the guiding principles and responsibilities to ensure St Stephen's House's security objectives are met.

2. Scope

This policy is applicable across St Stephen's House and individually applies to:

- all individuals who have access to St Stephen's House information and technologies;
- all facilities, technologies and services that are used to process St Stephen's House information;
- information processed, in any format, by St Stephen's House pursuant to its operational activities;
- internal and external processes used to process St Stephen's House information; and
- external parties that provide information processing services to St Stephen's House.

3. Objectives

St Stephen's House's objectives for information security are that:

- a culture is embedded to ensure all teaching, research and administration activities consider information security;
- individuals are aware and kept informed of their information security responsibilities;
- information risks are identified, managed and mitigated to an acceptable level;
- authorised users can securely 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.

4. Information Security Policy Framework (ISPF)

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

- all staff 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 St Stephen's House 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 St Stephen's House 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 St Stephen's House information assets, 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, St Stephen's House will implement 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 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 will support St Stephen's House in achieving its information security objectives. The policy and the baseline shall be communicated to users and relevant external parties, and available as a public document on the College website.

5. Responsibilities

The following bodies and individuals have specific information security responsibilities:

- **The Principal** is accountable for the effective implementation of this information security policy, and supporting information security rules and standards, within St Stephen's House.
- **House Council, as Governing Body** has executive responsibility for information security within St Stephen's House. Specifically, House Council has responsibility for overseeing the management of the security risks to St Stephen's House's staff and students, its infrastructure and its information.
- **The Data Controller** is responsible for establishing and maintaining St Stephen's House's information security management framework to ensure the availability, integrity and confidentiality of St Stephen's House's information. The Data Controller will lead on the definition and implementation of St Stephen's House's information security arrangements.
- **Users** are responsible for making informed decisions to protect the information that they process.

6. Compliance

St Stephen's House 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 will be treated extremely seriously by St Stephen's House and may result in enforcement action on a group and/or an individual.

7. Review and Development

This policy, and supporting ISPF documentation, shall be reviewed and updated by the Data Controller and approved by Governing Body on an annual basis to ensure that they:

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

Part 2 – Data Protection

1. Introduction

St Stephen's House is fully committed to compliance with the requirements of the Data Protection Act 1998 (DPA), which came into force on 1 March 2000, and to the General Data Protection Regulation 2016 (GDPR), which comes into force on 25 May 2018. The GDPR replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States. Its purpose is to protect the 'rights and freedoms' of natural persons (ie living individuals) and to ensure that personal data is not processed without their knowledge, and wherever possible, that it is processed with their consent. The College subscribes fully to the University's policy on Data Protection, available at: http://www.admin.ox.ac.uk/councilsec/dp/policy.shtml

We are required to maintain certain personal data about individuals for the purposes of satisfying our operational and legal obligations. We recognise the importance of correct and lawful treatment of personal data, as it helps to maintain confidence in our organisation and to ensure efficient and successful outcomes when using this data.

The types of personal data that we may process include information about current, past and prospective employees; students and academic visitors; clients and customers; suppliers and other organisations with whom we have dealings. Personal data may consist of any kind or format of information kept on paper, computer or other electronic media, all of which is protected under the DPA, and GDPR. For our full list of policies on the handling of information, please see our public website at: https://www.ssho.ox.ac.uk/about/policies/gdpr-2018.html

2. Principles

We endorse and adhere to the eight principles of the several Data Protection Acts, which are summarised as follows. Data must:

- 1. be processed fairly, transparently and lawfully and shall not be processed unless certain conditions are met.
- 2. be obtained for an explicitly specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- 3. be adequate, relevant and not excessive for those purposes.
- 4. be accurate and, where necessary, kept up-to-date.
- 5. only be kept for as long as is necessary for the purpose for which it was obtained.
- 6. be processed in accordance with the data subject's rights.
- 7. be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measure.
- 8. not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

These principles apply to obtaining, handling, processing, transportation and storage of personal data. Employees and agents of the College who obtain, handle, process, transport and store personal data for use must adhere to these principles at all times. Further, the GDPR requires that the College as data controller, can demonstrate compliance with the accountability principle, with proper documentation of process and data retention.

3. Types of data

Data Protection legislation lays down conditions for the processing of any personal data, and makes a distinction between personal data and "sensitive" personal data.

Personal data is defined as information relating to a living individual who can be identified from that data; or from that data and other information which is in the possession of, or is likely to come into the possession of the data controller, and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal information regarding an individual's racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; or criminal proceedings or convictions.

4. Handling of personal/sensitive information

The College will, through appropriate management and the use of strict criteria and controls:

- observe fully the conditions concerning the fair collection and use of personal information.
- specify the purpose for which information is used.
- collect and process information only to the extent that it is needed to fulfil operational needs or legal requirements.
- endeavour always to ensure the quality of information used.
- not keep information for longer than required operationally or legally.
- always endeavour to safeguard personal information by physical and technical means (i.e. keeping paper files and other records or documents containing personal/sensitive data in a secure environment; protecting personal data held on computers and computer systems by the use of secure passwords, which where possible, are changed periodically and ensuring that individual passwords are not easily compromised).
- ensure that personal information is not transferred abroad without suitable safeguards.
- ensure that the lawful rights of people about whom the information is held can be fully exercised.

In addition, the College will ensure that:

- there is someone with specific responsibility for data protection in the organisation (the designated Data Protection Officer) as defined within the GDPR.
- all employees managing and handling personal information understand that they are contractually responsible for following good data protection practice.
- all employees managing and handling personal information are appropriately trained.
- all employees managing and handling personal information are appropriately supervised.
- a clear procedure is in place for anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, and that such enquiries are promptly and courteously dealt with.
- methods of handling personal information are regularly assessed and evaluated.
- data sharing is carried out under a written agreement, setting out the scope and limits of the sharing.
- any disclosure of personal data will be in compliance with approved procedures.

Note that, by law, St Stephen's House has to provide employee liability information to any organisation that our employees are transferring to, in line with the Transfer of Undertakings Regulations.

5. Access to personal data

All individuals who are the subject of personal data held by us are entitled to:

- ask what information we hold about them, to whom it has been disclosed, and why.
- ask how to gain access to it.
- be informed how to keep it up-to-date.
- ask to have their personal data transmitted or migrated to another data controller.
- have personal data corrected where inaccurate, or removed entirely.
- prevent us from processing information or request that it is stopped if the processing of such data is likely to cause substantial, unwarranted damage or distress to the individual or anyone else.
- prevent us from processing information where the data is used for direct marketing.
- require us to ensure that no decision which significantly affects an individual is solely based on an automated process for the purposes of evaluating matters relating to him/her, such as conduct or performance.
- be informed what we are doing to comply with our legislated obligations.

This right is subject to certain exemptions which are set out in the DPA and GDPR. Any person who wishes to exercise this right should make the request in writing to the Data Protection Officer, or to the Bursar, in accordance with our published Subject Access Request process. If personal details are inaccurate, they will be amended upon request. If by providing this information we would have to disclose information relating to or identifying a third party, we will only do so provided the third party gives consent, otherwise we may edit the data to remove the identity of the third party.

Personal information will only be released to the individual to whom it relates. The disclosure of such information to anyone else without their consent may be a criminal offence. Any employee who is in doubt regarding a subject access request should check with the Data Protection Officer. Information must under no circumstances be sent outside of the EU without the prior permission of the Data Protection Officer.

We aim to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a written request unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

6. Employee responsibilities

All employees must ensure that, in carrying out their duties, St Stephen's House is able to comply with its obligations under the Data Protection legislation and any other legislation that applies. In addition, each employee is responsible for:

- checking that any personal data that he/she provides to us is accurate and up to date.
- informing us of any changes to information previously provided, e.g. change of address.
- checking any information that we may send out from time to time, giving details of information that is being kept and processed.

- if, as part of their responsibilities, employees collect information about other people or about other employees they must comply with this policy. This includes ensuring the information is processed in accordance with the DPA, is only processed for the purposes for which it is held, is kept secure, and is not kept any longer than is necessary.

Employees are reminded that the DPA does not just apply to records held relating to our employees, but also to any client files/records. Information stored on clients should be reviewed regularly to ensure it is accurate and up to date.

All documents, whether hand written or stored in emails (current or deleted) are potentially disclosable in the event of a request from an employee or client.

7. Data security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All employees are responsible for ensuring that any personal data that they hold is kept securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

- All personal data should be accessible only to those who need to use it, and access may only be granted in line with the College's Information Security Policy.
- Manual and paper records must not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation from either the Data Protection Officer or the College Bursar.
- Personal data may only be deleted or disposed of in line with the Records of Processing Activities (ROPAs) as published on the public website. Paper records that have reached their retention date are to be shredded and disposed of as 'confidential waste'.

8. Publication of information

Information that is already in the public domain is exempt from the Data Protection Acts. This would include, for example, information on employees contained within externally circulated publications such as brochures and other sales and marketing aids. Any individual who has good reason for wishing details in such publications to remain confidential should contact the Bursar or Data Protection Officer.

9. Subject consent

The need to process data for normal purposes will be communicated to all data subjects.
Our contracts of employment require the consent of employees to the processing of personal data for the purposes of administering, managing and employing our staff. This includes: payroll, benefits, medical records, absence records, sick leave/pay information, performance reviews, disciplinary and grievance matters, pension provision, recruitment, family policies (maternity, paternity, adoption, etc.) and equal opportunities monitoring.

In some cases, if the data is sensitive, for example information about health, race or gender, express consent to process the data will be obtained. Such processing may be necessary to comply with some of our policies, such as health and safety and equal opportunities.

Information about an individual will only be kept for the purpose for which it was originally given. Employees and managers must not collect data that is simply "nice to have" or which is to be used for another purpose.

10. Retention and disposal of data

Information will be kept in line with our document retention guidelines. All employees are responsible for ensuring that information is not kept for longer than necessary. Documents containing any personal information will be disposed of securely, and paper copies will be shredded.

11. Registration

St Stephen's House is registered in the Information Commissioner's public register of data controllers.
The Data Protection Act 1998 requires every data controller who is processing personal data to notify and renew their notification on an annual basis. Failure to do so is a criminal offence.

The College's Data Controller is responsible for ensuring compliance with the Data Protection Act, for notifying and updating the Information Commissioner of our processing of personal data, and for the monitoring and implementation of this policy on behalf of St Stephen's House.

Any changes made to the information stored and processed must be brought to the attention of the Data Controller immediately.

12. Implementation, monitoring and review of this policy

This policy has been in effect from 25 September 2017. The House Council of the College has overall responsibility for implementing and monitoring this policy, which will be reviewed on a regular basis (at least annually) following its implementation and additionally whenever there are relevant changes in legislation or to our working practices. It has been reviewed and substantially modified further to the Data Protection Act of 2018 (GDPR implementation).

Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the IT Manager.

This policy is not contractual, but indicates how St Stephen's House intends to meet its legal responsibilities for data protection. Any breach will be taken seriously and may result in formal disciplinary action. Any employee who considers that the policy has been breached in any way should raise the matter with the Data Protection Officer, the Bursar, or College Principal.

This document, and any future revision thereof, is posted on the main public College website at:
https://www.ssho.ox.ac.uk/about/policies/gdpr-2018.html