Issue Date:	June 2018
Approved by:	Approved by the Executive on 5 September 2018
Review Date:	June 2019

POLICY STATEMENT NO. 50

TITLE: **Data Protection (GDPR) Policy**

INTRODUCTION/OVERVIEW:

The General Data Protection Regulation (GDPR) forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The main provisions of this came into force, like the GDPR, on 25 May 2018.

The GDPR regulates the processing of personal data, and protects the rights and privacy of all individuals, for example, by giving all individuals who are the subject of personal data the right to gain access to their information; this is commonly referred to as subject access. Individuals can make a subject access request either verbally or in writing. Data includes paper/manual files; electronic records; photographs; CCTV images, and may include facts or opinions about a person.

Please see the Data Protection Data Sharing Code of Practice, published by the Information Commissioner's Office (ICO) for further details (www.ico.og.uk).

STATEMENT/ GUIDELINES

1. **Purpose**

The College is committed to protecting the rights and privacy of individuals, including students, staff and others, in accordance with the General Data Protection Regulations (GDPR) May 2018.

The new regulation demands higher transparency and accountability in how personal data is used and managed.

The GDPR contains provisions that the College must be aware of as a data controller, including provisions intended to enhance the protection of personal data. For example:

College privacy notices are concise and transparent, and written in clear and plain language.

The College needs to process certain information about its staff, students, and other individuals with whom it has a relationship for various purposes such as:

- recruitment and payment of staff
- administration of all courses
- recording of learner progress
- collection of fees
- claiming and recording of achievement
- processing of bursary, free school meals, learning and learner support
- complying with legal obligations to funding bodies and the government

(This is not an exhaustive or definitive list).

Personal data is defined broadly and covers such things as name, address, email address, IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs, health, sexual orientation and criminal records. These more sensitive types of personal data are called 'Special Categories of Personal Data' and are given additional protection by data protection laws.

To comply with various legal obligations, the College must ensure that all information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

2. **Compliance**

This policy applies to all personnel including employees, consultants, contractors and temporary personnel at the College. Any breach of this policy or the Regulations itself will be considered as an offence and the College's disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with the College and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments who are responsible for dealing with external bodies e.g. subcontracting partners, cloud storage providers, will take responsibility for ensuring that they sign a contract which includes an agreement to confirm that they have read and will abide by this policy.

This policy will be updated as and when required, to reflect any changes or amendments made to General Data Protection Regulations May 2018 or other relevant legislations.

3. **Responsibilities**

The College will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data.

The College has appointed a Data Protection Officer (DPO), who is also the Director of IT & Resources, who can be contacted via email at dpo@stamford.ac.uk who is available to address any concerns regarding data held by the College and how it is processed, held and used.

The DPO is responsible for all day-to-day data protection matters, and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for ensuring good practice regarding the handling of data within the College.

The Data Protection Officer is also responsible for ensuring that the College's notification process is timely and accurate. Information about this can be found on Information Commissioner's Office website https://www.gov.uk/notification-to-process-personal-data. Our data registration number is **Z4665294**

All college personnel are personally responsible for complying with the legislation regarding the processing of personal information.

Individuals who provide personal data to the College are responsible for ensuring that the information submitted is accurate and up-to-date.

All staff responsible for collecting and sharing candidates' data are required to follow strict rules called 'data protection principles' ensuring the information 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 (refer to Retention Policy)
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

College personnel must not release or disclose any personal data outside the College or inside the College to College personnel not authorised to access the personal data without authorisation from their manger or the DPO (this includes telephone calls and emails). College personnel must take steps to ensure there is no unauthorised access to personal data whether by College personnel who are not authorised to see such personal data, or by people outside the College.

4. **Data Protection Principles**

The College is required by law to process any personal data in accordance with the following eight principles:

1. Ensure that all personal data shall be processed fairly and lawfully and, in particular, shall not be processed without informing the data subject, where possible, the identity of the data controller, the reason for collecting and processing the data, informing them of any third party who has access to the data, indicate the length of time the data will be held for, and any other information deemed necessary to disclose.

2. Only use the data for the purpose for which is was originally collected, unless the data subject is informed prior to any additional processing.

3. Ensure that the data collected is adequate, relevant and not excessive. Any data that is not strictly necessary must be destroyed immediately.

4. Review and update personal data to keep it as accurate as possible. It is the responsibility of the individual to inform the College of any changes to their circumstance that requires data to be amended. The College must act on any changes without delay.

5. To ensure compliance with GDPR legislation, the College must have a clear Data Retention Policy. The College must not retain any personal data for any longer than is necessary, or as detailed in our retention policy.

   The College will ensure that all personal data is disposed of in a way that protects the privacy of the data subject e.g. using secure confidential waste systems, electronic deletion, etc. A log will be kept of records that are destroyed.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall 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.

5. **Lawful Basis for Processing Data**

The College is required to have a valid lawful basis in order to process personal data. There are six lawful bases for processing data. Our privacy notice must include the lawful basis for processing the data as well as the purpose for processing the data:

a) Consent: the individual has given clear consent for the College to process their personal data for a specific purpose.

b) Contract: the processing is necessary for a contract the College has with the individual, or because they have asked the College to take specific steps before entering into a contract. The College must require this data to fulfil their contractual obligation.

c) Legal obligation: the processing of data is necessary for the College to comply with a common law or statutory obligation, but not including contractual obligations.

d) Vital interests: the processing is necessary to protect someone's life.

e) Public task: the processing is necessary for the College to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

f) Legitimate interests: the processing is necessary for the legitimate interest of the College or a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interest.

The College will ensure that any forms used to collect data from an individual will contain a statement explaining the lawful basis for processing the data, what the data will be used for and who the data will be shared with, if applicable.

In addition, when the College collects or uses special categories of personal data, the College will met the additional conditions set out in the GDPR.

For individuals who do not give permission for the processing of their data, and where the data cannot be processed under another lawful basis, the College will take steps to ensure that the processing of this data does not take place.

6. **Subject Access Request**

An individual has the right to request access to, or copies off, all personal data held by the College relating to them. All Subject Access Requests must be made in writing to the Data Protection Officer at the College.

Please see our separate Subject Access Request policy for further information. All requests will be dealt with within a month of receipt.

7. **Sharing of Data/Third Party Access**

The College will only share data that has been notified under the Data Protection Notification, and that the individual has been made aware off. Staff must not disclose data held on another person or a third party.

The College must obtain ID to verify the identity of the person requesting personal data.

In the case of looked-after children or those in care, agreements may already be in place for information to be shared with the relevant authorities, for example, the Local Authority. The College's Data Protection Officer will confirm the status of these agreements and approve/reject any requests.

The College may legitimately share data in the following circumstances:

- the data subject has given consent for the data to be shared
- a notification of disclosure has been received and is in the legitimate interest of the College
- the College is obliged, by law, to disclose the information
- the data is needed for the College to fulfil its contractual obligation in the interests of safeguarding concerns

Under no circumstances will the College sell any of its data to a third party.

8. **Data Retention Period**

Details of retention periods, the actions taken at the end of the retention period and method of disposal are contained in the College's Data Retention Policy which is available/accessible from the Data Protection Officer, or via our website.

9. **Data Breach**

Please see our GDPR Data Breach Policy and Procedure at Appendix A for further information which is also available/accessible from the Data Protection Officer, or via our website.

10. **Emails**

The College must ensure that all individuals either sending or receiving emails at college are made aware that the content may be disclosed if a request for information is made. This is in line with Data Protection and Freedom of Information Legislation.

Any email sent to or from the College may be accessed by someone other than the intended recipient for security or management purposes. This is in line with the Lawful Business Practice Regulations and the Regulation of Investigatory Powers Act 2000.

11. **CCTV**

CCTV systems are in operation on College premises. This is to protect College staff, students, visitors, members of the public and property. Any images obtained from the CCTV system will be processed in accordance with legislation.

IMPACT ASSESSMENT:

This policy has been assessed and considered for impact upon people who share the following protected characteristics and factors: race, gender and gender identity, disability (including learning difficulty), religion and belief, sexual orientation, age, pregnancy, maternity and marital status.

EQUALITY IMPACT ASSESSMENT SUMMARY:

This policy has been impact assessed and has identified the following:

- Negative impacts (Y)

- Appropriate actions/mitigations to address the negative impacts have been put in place (Y)
- Positive impacts (Y)

For further detail of the impacts and associated actions, please see the EIA which is attached to the filed copy of this document.

LINKED POLICIES:

Data Retention Policy

MONITORING PROCEDURE:

DATE FOR REVIEW:

June 2019

RESPONSIBILITY:

Director of IT & Resources (Data Protection Officer)

ENDORSED BY EXECUTIVE:

Principal *Janet Meenaghan*

Date 5 September 2018

Appendix A

DATA BREACH POLICY & PROCEDURE

1.0 Introduction

1.1 New College Stamford holds, processes, and shares a large amount of personal data, a valuable asset that needs to be suitably protected.

1.2 Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

1.3 Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or fines under General Data Protection Regulations (GDPR).

2.0 Purpose

2.1 The College is obliged under the Data Protection Act and GDPR to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

2.2 This policy sets out the procedure to be followed to ensure a consistent and effective approach for managing data breach and information security incidents across the College.

3.0 Scope

3.1 This policy relates to all personal and sensitive data held by the College regardless of format.

3.2 This policy applies to all staff and students at the College including temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the College.

3.3 The objective of this policy is to contain any breaches, to minimise the risk associated with the breach, to appropriately report the breach and consider what action is necessary to secure personal data and prevent further breaches.

4.0 Definition / Types of Breach

4.1 For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

4.2 A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

An incident, in the context of this policy, is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused, or has the potential to cause, damage to the College's information assets and/or reputation.

4.3 An incident includes, but is not restricted to, the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)
- Equipment theft or failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data
- Hacking attack
- Unforeseen circumstances such as a fire or flood resulting in data loss
- Human error
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

5.0 Reporting an incident

5.1 Any individual who accesses, uses or manages the College's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer (DPO) via the IT Services helpdesk (at itsupport@stamford.ac.uk)

5.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

5.3 The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process (see Appendix A)

6.0 Containment and Recovery

6.1 The (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

6.2 An initial assessment will be made by the DPO in liaison with relevant officers to establish the severity of the breach and who will lead the investigation into the breach (this will depend on the nature of the breach, in some cases it could be the DPO).

6.3 The Investigating Officer (IO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

6.4 The IO will establish who may need to be notified as part of the initial containment and will inform the police, supervisory authorities and individuals, dependent upon the level of risk to the rights and freedoms of individuals.

6.5 The IO, in liaison with the relevant officer(s), will determine the suitable course of action to be taken to ensure a resolution to the incident.

7.0 Investigation and Risk Assessment

7.1 An investigation will be undertaken by the IO immediately and, wherever possible, within 24 hours of the breach being discovered / reported.

7.2 The IO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

7.3 The investigation will need to take into account the following:

- the type of data involved
- its sensitivity
- that protections are in place (e.g. encryption)
- what has happened to the data, has it been lost or stolen
- whether the data could be put to any illegal or inappropriate use
- who the individuals are, number of individuals involved and the potential effects on those data subject(s)
- whether there are wider consequences to the breach under the GDPR

8.0 Notification

8.1 The Director of IT and the Principal will determine who needs to be notified of the breach.

8.2 In certain circumstances, the College is required to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed, such a breach is likely to have a significant detrimental effect on individuals, for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

8.3 A notifiable breach must be reported to the ICO within 72 hours of the College becoming aware of it.

8.4 Every incident will be assessed on a case by case basis, however, the following will need to be considered:

- whether there are any legal/contractual notification requirements;
- whether notification would assist the individual affected – could they act on the information to mitigate risks?
- whether notification would help prevent the unauthorised or unlawful use of personal data?
- where there is likely to be a risk to the freedoms of individuals, the Information Commissioner's Office (ICO) should be notified.

8.5 Notification to the individual(s) whose personal data has been affected, will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks. Individuals will also be provided with on how they can contact the College for further information or to ask questions on what has occurred.

8.6 The IO and or the DPO must consider notifying third parties such as the police, insurers, bank or credit card companies and trade unions. This would be appropriate

where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

8.7 The IO and or the DPO will consider whether the Head of Marketing, Deputy Principal Curriculum and Quality, Executive Office or Principal should be informed regarding a press release and to be ready to handle any incoming press enquiries.

8.8 All actions will be recorded by the DPO.

9.0 Evaluation and response

9.1 Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach, the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

9.2 Existing controls will be reviewed to determine their adequacy and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

9.3 The review will consider:

- where and how personal data is held and where and how it is stored
- where the biggest risks lie and will identify any further potential weak points within its existing measures
- whether methods of transmission are secure; sharing minimum amount of data necessary
- identifying weak points within existing security measures
- staff awareness
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security

9.4 If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered

APPENDIX A

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify your Head of Department immediately, complete Section 1 of this form and email it to the IT Helpdesk ITSupport@stamford.ac.uk

Section 1: **Notification of Data Security Breach**	**To be completed by Head of Department of person reporting incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please, provide details:	
Brief description of any action taken at the time of discovery:	

For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Investigating Officer in consultation with the Head of Department affected by the breach and, if appropriate, IT where applicable**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the College or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data □ **Sensitive personal data** (as defined in the Data Protection Act/GDPR) relating to an identifiable individual's a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) commission or alleged commission of any offence, or f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	
□ Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
□ Personal information relating to vulnerable adults and children;	

□ Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
□ Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
□ Security information that would compromise the safety of individuals if disclosed.	
Data Protection Officer and/or Investigating Officer to consider whether it constitutes a reportable data breach	

Section 3: Action taken	To be completed by Data Protection Officer and/or Investigating Officer
Incident number	**e.g. year/001**
Report received by:	
On (date):	
Action taken by responsible officer(s):	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow-up action required/recommended:	
Reported to Data Protection Officer and Lead Investigating Officer on (date):	
Reported to other internal stakeholders (details, dates):	
For use of Data Protection Officer and/or Lead Investigating Officer:	
Notification to ICO	**YES/NO If YES, notified on:** **Details:**
Notification to data subjects	**YES/NO If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder	**YES/NO If YES, notified on:** **Details:**