Policy No. GDPR01

Inspire Education Group

Data Protection (GDPR) Policy

Purpose

The Group 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 Group 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.

The purpose of this policy is to:

- enable the Group to demonstrate that it fully complies with General Data Protection Regulation 2018
- ensure that all staff and members of the Group are fully briefed on data protection issues
- inform staff of their responsibilities within the context of their job and show a line of responsibility towards implementing General Data Protection Regulation 2018 across the Group
- clearly define individual's rights with regard to processing personal data and accessing personal data within the context of the legislation
- Ensure that all personal data is stored securely
- give direction and guidance for dealing with requests to access personal data
- ensure that all staff are aware of the issues surrounding the disclosure of personal data
- set data retention periods for personal data
- inform staff of their responsibilities if a data breach, or near miss, occurs.

Scope

This policy applies to all personnel including employees, consultants, contractors and temporary personnel at the Group. Any breach of this policy or the Regulations itself will be considered as an offence and the Group's disciplinary procedures will be invoked.
As a matter of best practice, other agencies and individuals working with the Group 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.

The Policy Statement

1. Introduction

This Data Protection Policy has been developed to ensure that Inspire Education Group (the Group) fully complies with General Data Protection Regulation 2018. The policy emphasises the duties and obligations of every member of staff under General Data Protection Regulation 2018 and the codes of practice issued by the Information Commissioner. For the purposes of this Policy, the Group represents Peterborough College and Stamford College.

Compliance with General Data Protection Regulation 2018 is the responsibility of all members of the Group. Any deliberate breach of the Data Protection Policy may lead to disciplinary legislation being taken, access to Group facilities being withdrawn, or a criminal prosecution.

If there are any questions about the interpretation or operation of this policy, please contact the Data Protection Officer, Inspire Education Group, Park Crescent, Peterborough PE1 4DZ, email rob.cottrell@stamford.ac.uk

2. Risk Analysis

The maximum penalty for failing to comply with General Data Protection Regulation 2018 is the greater of 10 million Euros or 2% of the Group's annual turnover. The reputation of the Group may also be damaged by non-compliance with this policy.

The risk of non-compliance is monitored in accordance with the Group's Risk Management Policy. Where there is a high risk that the rights and freedoms of individuals may be infringed, a Data Protection Impact Assessment will be undertaken.

3. Responsibilities

The Group 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 Group has appointed a Data Protection Officer (DPO), who 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 Group.

The Data Protection Officer is also responsible for ensuring that the Group'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 **Z6337074**.

3.1 Staff

All staff are responsible for:

- checking that any information that they provide to Human Resources in connection with their employment is accurate and up-to-date
- informing Human Resources of any changes to information which they have provided i.e. change in address, telephone number, etc

- checking the information that the Group will send out annually, giving details of information kept and processed about staff
- informing the Group of any errors or changes. The Group cannot be held responsible for any errors unless the staff member has informed Human Resources.

In addition, all staff are responsible for:

- processing personal data as required by their job role in accordance with General Data Protection Regulation 2018
- ensuring that any personal data for which they are responsible is kept securely
- ensuring that personal information is not disclosed, whether orally, in writing, accidentally or otherwise, to any unauthorised third party
- reporting any personal data breach, or circumstances which could potentially give rise to a personal data breach, to the Data Protection Officer immediately.

Personal information should be:

- kept in a locked room (i.e. a locked staff room)
- in a locked filing cabinet
- in a locked drawer
- if it is computerised, be password protected or stored only on a device which is encrypted.

The IT Support Unit (ITSU) is responsible for ensuring that the Group network is protected against malware and for encrypting all laptops and storage devices issued to staff.

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen- savers and manual records should not be left where they can be accessed by unauthorised personnel.

This policy also applies to staff and students who process personal data off-site. Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and students should take particular care when processing personal data at home or in other locations outside the Group's campuses.

3.2 **Student Obligations**

Students must ensure that all personal data provided to the Group is accurate and up-to-date. They must ensure that changes of address etc. are notified to the Course Tutor who then must fill in the appropriate form. Students who use the Group computer facilities may, from time to time, process personal data. If they do, they must notify the Data Protection Officer. Any student who requires further clarification about this should contact their Course Tutor in the first instance.

3.3 **Registration with the Information Commissioner**

The Group is registered with the Information Commissioner and has an obligation as a Data Controller to notify the Information Commissioner of the purposes for which it processes personal data. Personal data must only be processed if the purpose for which it is required has been 'notified' to the Information Commissioner. It is a criminal offence to hold personal data that has not been registered.

A list of purposes, which have been registered by the Group, is as follows:

Purpose 1	Staff, Agent and Contractor Administration
Purpose 2	Advertising, Marketing, Public Relations, General Advice Services
Purpose 3	Accounts and Records
Purpose 4	Education

Purpose 5 Student and Staff Support Services
Purpose 6 Crime Prevention and Prosecution of Offenders
Purpose 7 Provision of facilities to other groups or organisations
Purpose 8 Publication of the Group's magazines

Managers are expected to familiarise themselves with the terms of the Group's register entry. If any doubt exists as to whether any particular collecting, holding and use, or intended disclosure of personal data is within the terms of the Group's register entry or General Data Protection Regulation 2018, then staff must discuss this with the Data Protection Officer before taking action. Senior members of staff should keep the Data Protection Officer informed of non-standard data held in their areas.

Individual data subjects can obtain full details of the Group's data protection register entry with the Information Commissioner from the Group Data Protection Officer or from the Information Commissioner's website (https://ico.org.uk/).

4. Definitions

For the purposes of this Policy the following definitions shall apply;

- "personal data" shall mean any information relating to an identified or identifiable natural person (the "data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
- "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction
- "personal data filing system" ("filing system") shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis
- "controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law
- "processor" shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
- "the Group" shall mean Inspire Education Group.

5. Principles Relating to the Processing of Personal Data

5.1 Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation')
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ('storage limitation')
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

5.2 The Group, as data controller, shall be responsible for, and be able to demonstrate compliance with the principles above ('accountability').

6. The Rights of Individuals

6.1 The right to be informed

General Data Protection Regulation 2018 sets out the information that must be supplied to individuals whose personal data the Group holds and when those individuals should be informed. Further details may be obtained from the Group's Data Protection Officer.

The information that the Group supplies about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible
- written in clear and plain language, particularly if addressed to a young person
- free of charge.

6.2 The right of access

Under General Data Protection Regulation 2018, individuals have the right to obtain:

- confirmation that their data is being processed
- access to their personal data
- other supplementary information.

Access requests should be made to the Group's Data Protection Officer in writing. The Group will provide one copy of the information free of charge. However, we may charge a reasonable fee when a request is manifestly unfounded or excessive, particularly if it is repetitive.

6.3 The right to rectification

Individuals are entitled to have personal data held by the Group rectified if it is inaccurate or incomplete. Requests for rectification of data should be made to the Group's Data Protection Officer in writing who will respond within one month. This may be extended by two months where the request for rectification is complex.

6.4 The right to erasure

Individuals have a right to have their personal data erased and to prevent processing in specific circumstances. Requests for data to be erased should be made to the Group's Data Protection Officer in writing.

There are some specific circumstances where the right to erasure does not apply and the Group may refuse to deal with a request.

6.5 The right to restrict processing

Individuals have the right to restrict the processing of their personal data in the following circumstances:

- the accuracy of the personal data is contested by the individual, for a period enabling the Group to verify the accuracy of the personal data
- the processing is unlawful and the individual opposes the erasure of the personal data and requests the restriction of their use instead

- the Group no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims
- the individual has objected to processing pending verification whether the legitimate grounds of the Group override those of the individual.

Requests to restrict the processing of data should be made to the Group's Data Protection Officer in writing.

6.6 **Data portability**

The Group will provide personal data in a structured and commonly used format. We will also transmit personal data directly to another organisation if requested by the data subject.

6.7 **The right to object**

An individual has the right to object;

- where the lawful basis for processing the personal data of an individual is based solely on the legitimate interests of the Group or the performance of a task in the public interest, or the exercise of an official authority vested in the Group, on grounds relating to his or her particular situation
- to the use of their personal data for direct marketing.

Objections to the processing of personal data under this section should be notified to the Data Protection Officer in writing.

The Group will not process personal data for the purposes of scientific or historical research and statistics.

6.8 **Automated decision making and profiling**

The Group will not undertake automated decision making or process personal data for the purpose of profiling individuals.

7. Consent of the Data Subject

The Group will identify and record a lawful basis for the processing of personal data.

The lawful basis for the processing of personal data will normally be the consent of the data subject. Consent must be a freely given, specific, informed and unambiguous indication of the individual's wishes. Consent will not be inferred from silence, pre-ticked boxes or inactivity. Consent is not required if a different lawful basis has been identified (see following section).

Individuals may withdraw their consent for the processing of their personal data by notifying the Data Protection Officer in writing.

8. Other Lawful Bases for Processing Personal Data

Having regard to the purpose of the data processing and the relationship with the individual, the Group may determine that it is not appropriate to obtain the consent of the data subject and may instead identify and document one of the following lawful bases for the processing of personal data;

- the processing is necessary for a contract between the Group and the individual, or because the individual has asked the Group to take specific steps before entering into a contract
- the processing is necessary for the Group to comply with the law, for example, The Further and Higher Education Act 1998
- the processing is necessary to protect someone's life
- the processing is necessary for the Group to perform a task in the public interest or to discharge its official functions, and the task or function has a clear basis in law

- the processing is necessary for the legitimate interests of the Group or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests (this does not apply if the Group is processing data to perform its official tasks).

9. Processing of Data on Criminal Convictions

In order to comply with statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Group obtains details of criminal allegations, proceedings and convictions for the purpose of safeguarding the young people and vulnerable adults for which it is responsible. This data is only retained for as long as required for this purpose and is then deleted. The Group does not keep a comprehensive register of criminal convictions.

10. Privacy Notices, Transparency and Control

The Group aims to comply with the code of practice on communicating privacy information to individuals issued by the Information Commissioners' Office.

Privacy notices will be as informative as possible and will, as a minimum, inform individuals;

- that the Group is the data controller
- how their personal data will be used by the Group and
- with whom their data will be shared.

Privacy information will be given before personal data is collected and may be communicated through a variety of media;

- in writing - forms, such as application forms; printed media; printed adverts
- electronically - on the Group's websites; in emails; in text messages; in mobile apps
- orally - face to face or when speaking on the telephone (this will be documented)
- through signage - for example an information poster in a public area.

11. Data Protection Impact Assessment

The Group aims to comply with the code of practice on conducting privacy impact assessments issued by the Information Commissioners' Office.

Risks created by the Group's data processing activities are continuously monitored through the Group's risk register in order to identify when a type of processing is likely to result in a high risk to the rights and freedoms of individuals. This is most likely when any of the following conditions are present;

- sensitive data or data of a highly personal nature
- data concerning vulnerable data subjects
- data processed on a large scale
- applying new technological or organisational solutions.

Where the likelihood that the rights and freedoms of individuals may be infringed is assessed as 'High' or above (using the Group's methodology for scoring risks), the Data Protection Officer will arrange for a Data Protection Impact Assessment to be undertaken. The Data Protection Impact Assessment will incorporate the following steps;

- describe the information flows
- identify the privacy and related risks
- identify and evaluate the privacy solutions
- sign off and record the assessment outcomes
- integrate the outcomes into the existing processes or project plan
- consult with internal and external stakeholders as needed throughout the process.

12. Data Sharing

The Group aims to comply with the code of practice on data sharing issued by the Information Commissioners' Office.

The Group will inform an individual if is intended to share his or her personal data with another organisation and will normally obtain the consent of individual.

The Group does not require the consent of a student to share his or her personal data for the purpose on complying with:

- its contractual obligations to the Education and Skills Funding Agency and successor organisations
- its legal obligations under the education acts and safeguarding legislation.

The Group may share personal data without the individual's knowledge, where, for example, personal data is processed for the:

- prevention or detection of crime
- apprehension or prosecution of offenders or
- assessment or collection of tax or duty.

The Group will share personal data with its service providers to the minimum extent required for those service providers to discharge their obligations to the Group under relevant service contracts. Service providers includes auditors, payroll providers, bankers, debt collection agencies, software suppliers and providers of grant funding.

The Group will not transfer personal data outside the European Union.

13. Retention of Data

The Group will retain data in a form which permits the identification of data subjects for no longer than the purposes for which the data are processed. The retention periods for each class of data are shown in Appendix 1.

14. Personal Data Breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This is more than a loss of personal data. All personal data breaches, or circumstances which may give rise to a personal data breach, must be reported to the Data Protection Officer immediately.

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.

15. Closed Circuit Television (CCTV)

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

16. Examinations

16.1 Examination scripts

Examination scripts are expressly exempted from the data subject access rules. This means that the Group is under no obligation to permit examination candidates to have access to either original scripts or copies of the scripts.

16.2 **Disclosure of examination results**

Examination results (including other forms of assessment such as coursework marks, module marks, and phase tests) are personal data and, therefore, should not be disclosed to third parties without consent.

16.3 **Internal and external examiners' comments**

A data subject has the right to request a copy or summary 'in intelligible form' of internal and external examiners' comments, whether made on the script or in another form that allows them to be held and applied to the original script or to a specific candidate within 40 days.

17. Emails

The Group must ensure that all individuals either sending or receiving emails at the Group premises 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 Group 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.

18. Complaints

Any person who believes that the Group has not complied with this Policy, or with any aspect of the wider General Data Protection Regulation 2018, should notify the Group's Data Protection Officer in the first instance. If the issue is not resolved, a complaint should be made in writing to the Group Chief Executive Officer and will be investigated in accordance with the Group's Complaints and Dissatisfactions Resolution Procedure, a copy of which may be obtained from any of the Group's Receptions.

If the complainant is still unhappy with the Group's response or needs any advice he or she should contact the Information Commissioner's Office (ICO) on the ICO helpline (telephone: 0303 123 1113) or go to the Information Commissioner's website at https://www.gov.uk/data-protection/make-a-complaint.

Related Procedures and Documentation

GDPR Data Breach Policy and Procedure (Appendix A)
Data Breach Report Form (Appendix B)

Responsibility

This policy is the responsibility of the Data Protection Officer

Date of Last Review July 2020

Appendix A

DATA BREACH POLICY & PROCEDURE

1. Introduction

1.1 Inspire Education Group (the Group) 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. Purpose

2.1 The Group 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 Group.

3. Scope

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

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

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. 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 Group'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. Reporting an Incident

5.1 Any individual who accesses, uses or manages the Group'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 B).

6. Containment and Recovery

6.1 The Data Protection Officer (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. 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. Notification

8.1 The Director of IT and either the Group Chief Executive Officer or the Deputy Chief Executive Officer will determine who needs to be notified of the breach.

8.2 In certain circumstances, the Group 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 Information Commissioner's Office (ICO) within 72 hours of the Group 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 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 Group 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, Vice 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. 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.

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 Group 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 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:**