



# Choices Academy

## GDPR Policy



Version	Purpose/change	Author	Date	Review date:
1	V1 approved	Sarah Howe	16/11/2023	16/11/2024



# Choices Academy

## CONTENTS

<b>Topic number</b>	<b>Topic</b>	<b>Page</b>
	<b>Purpose and scope</b>	<b>3</b>
	<b>Policy statement</b>	<b>4</b>
<b>1.</b>	<b>Responsibilities – staff and students</b>	<b>4, 5 &amp; 6</b>
<b>2.</b>	<b>Related documentation</b>	<b>5</b>
<b>Appendices</b>		
<b>Appendix 1</b>	<b>Data Protection (GDPR) Policy –Data Protection Obligations</b>	<b>7-13</b>
<b>Appendix 2</b>	<b>Data Protection (GDPR) Policy – Data Breach Policy &amp; Procedure</b>	<b>14- 17</b>
<b>Appendix 3</b>	<b>Data Protection (GDPR) Policy – Data Breach Report Form</b>	<b>18-21</b>



# Choices Academy

## **Purpose**

Choices Academy 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. Failure to comply with the GDPR is a financial risk and reputational risk for the Academy. The Academy 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 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 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.

## **Scope**

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



# Choices Academy

## The Policy Statement

To ensure the Academy can demonstrate that it fully complies with General Data Protection Regulation 2018 the academy will:

- Ensure all staff and members of the academy 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 regarding 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 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
- Monitor risk of non-compliance in accordance with the Group's Risk Management Policy
- Undertake Data Protection Impact Assessment where there is a high risk that rights and freedoms of individuals may be infringed

## 1. Responsibilities

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of the Data Protection Policy may lead to disciplinary legislation being taken, access to academy facilities being withdrawn, or a criminal prosecution.

The academy 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 Academy 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 Choices Academy GDPR Director will manage GDPR compliance for the Academy. The Data Protection Director is also responsible for ensuring that the Group's notification process is timely and accurate. Information about this can be found on the Information Commissioner's Office website <https://www.gov.uk/notification-to-process-personal> data. **Our data registration number is: 00012203567.**



# Choices Academy

## 1.2 Staff

All Staff are responsible for:

- Checking that any information that they provide to Management in connection with their employment is accurate and up to date
- Informing Management of any changes to information which they have provided i.e., change in address, telephone number, etc
- Checking the information that the Academy will send out annually, giving details of information kept and processed about staff
- Informing the Academy of any errors or changes. The Academy cannot be held responsible for any errors unless the staff member has informed Management

**In addition, all staff are responsible for:**

- Processing personal data as required by their job role in accordance with GDPR
- Ensuring any personal data for which they are responsible is kept securely
- Ensuring 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 or in a locked drawer
- Be password protected or stored only on a device which is encrypted if it is computerised

The IT Officer is responsible for ensuring that the Academy 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 unauthorised personnel can access them.

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 academy's offices.



# Choices Academy

## **1.3 Students**

- Students must ensure that all personal data provided to the academy 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 academy's computer facilities may, from time to time, process personal data. If they do, they must notify the Data Protection Director. Any student who requires further clarification about this should contact their Course Tutor in the first instance. If there are any questions about the interpretation or operation of this policy, please contact the Data Protection Director.

## **2. Related Documentation**

- Data Protection Obligations (Appendix 1)
- GDPR Data Breach Policy and Procedure (Appendix 2)
- Data Breach Report Form (Appendix 3)
- GDPR 2018
- Information Commissioner's Office Codes of Practice
- IEG Privacy Statement



# Choices Academy

## Data Protection (GDPR) Policy – Appendix 1 Data Protection Obligations

The Academy 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.

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

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

### 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 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



# Choices Academy

## **Principles Relating to the Processing of Personal Data**

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 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')

## **The Rights of Individuals**

### **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

### **Academy 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

### **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





# Choices Academy

- Other supplementary information Access requests should be made to the Academy's Data Protection Officer in writing.

The Academy 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.

## **The right to rectification**

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

## **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 Academy's Data Protection Director in writing. There are some specific circumstances where the right to erasure does not apply, and the Academy may refuse to deal with a request.

## **The right to restrict processing**

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

- The individual contests the accuracy of the personal data, for a period enabling the Academy 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 Academy 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 Academy override those of the individual Requests to restrict the processing of data should be made to the Academy's Data Protection Director in writing.

## **Data portability**

The Academy 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.

## **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 Academy or the performance of a task in the public interest, or the exercise of an official authority vested in the Academy, on grounds relating to his or her situation



# Choices Academy

- 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 Director in writing. The Academy will not process personal data for the purposes of scientific or historical research and statistics.

## **Automated decision making and profiling**

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

## **Consent of the Data Subject**

The Academy 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 Director in writing.

## **Other Lawful Bases for Processing Personal Data**

Having regard to the purpose of the data processing and the relationship with the individual, the Academy 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 Academy and the individual, or because the individual has asked the Academy to take specific steps before entering a contract
- The processing is necessary for the Academy 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 Academy 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 Academy 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 Academy is processing data to perform its official tasks)

## **Processing of Data on Criminal Convictions**

To comply with statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Academy 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 Academy does not keep a comprehensive register of criminal convictions.

## **Privacy Notices, Transparency and Control**



# Choices Academy

The Academy 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 Academy is the data controller
- How their personal data will be used by the Academy 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 - 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

## **Data Protection Impact Assessment**

The Academy aims to comply with the code of practice on conducting privacy impact assessments issued by the Information Commissioners' Office. Risks created by the Academy's data processing activities are continuously monitored through the Academy's risk register 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 Academy's methodology for scoring risks), the Data Protection Director 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



# Choices Academy

## **Data Sharing**

The Academy aims to comply with the code of practice on data sharing issued by the Information Commissioners' Office. The Academy will inform an individual if it is intended to share his or her personal data with another organisation and will normally obtain the consent of the individual. The Academy does not require the consent of a student to share his or her personal data for the purpose of complying with its:

- Contractual obligations to the Education and Skills Funding Agency and successor organisations
- Legal obligations under the education acts and safeguarding legislation

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

## **Retention of Data**

The Academy 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 set out in the Retention Policy.

## **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 Director immediately.

Please see our GDPR Data Breach Policy and Procedure at Appendix 2 for further information which is also available from the Data Protection Director.

## **Closed Circuit Television (CCTV)**

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



# Choices Academy

## **Examinations**

### **Examination scripts**

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

### **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.

### **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.

### **Emails**

The Academy must ensure that all individuals either sending or receiving emails at the Academy 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 Academy 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

### **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 Academy's Data Protection Director in the first instance. If the issue is not resolved, a complaint should be made in writing to the Academy Director and will be investigated in accordance with the Academy's Complaints Procedure. If the complainant is still unhappy with the Academy'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>.



# Choices Academy

## Data Protection (GDPR) Policy – Appendix 2 Data Breach Policy & Procedure

### Introduction

The Academy holds, processes, and shares a large amount of personal data, an asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security. 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).

### Purpose

The Academy 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. 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 Academy.

### Scope

This policy relates to all personal and sensitive data held by the Academy regardless of format. This policy applies to all staff and students of the Academy including temporary, casual or agency staff and contractors, consultants, suppliers, and data processors working for, or on behalf of the Academy. 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.

### Definition/Types of Breach

To this policy, data security breaches include both confirmed and suspected incidents.

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 Academy's information assets and/or reputation.

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



# Choices Academy

- 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

## **Reporting an Incident**

Any individual who accesses, uses, or manages the Academy's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. 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 3).

## **Containment and Recovery**

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.

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).

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.

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.

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.

## **Investigation and Risk Assessment**

The IO will undertake an investigation immediately and, wherever possible, within 24 hours of the breach being discovered / reported.



# Choices Academy

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.

The investigation will need to consider 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

## **Notification**

The Director and Management Team will determine who needs to be notified of the breach.

In certain circumstances, the Academy 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.

A notifiable breach must be reported to the Information Commissioner's Office (ICO) within 72 hours of the Academy becoming aware of it. 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

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 Academy for further information or to ask questions on what has occurred.





# Choices Academy

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.

The IO and/or the DPO will consider whether to issue a press release and to be ready to handle any incoming press enquiries.

All actions will be recorded by the DPO.

## **Evaluation and Response**

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.

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.

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



# Choices Academy

## Data Protection (GDPR) Policy – Appendix 3 Data Breach Report Form

Please act promptly to report any data breaches. If you discover a data breach, please notify your Manager immediately, complete Section 1 of this form and email it to the Data Protection Director

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



# Choices Academy

**For use by the Data Protection Officer**

<b>Received by:</b>	
<b>On (date):</b>	
<b>Forwarded for action to:</b>	
<b>On (date):</b>	

<b>Section 2: Assessment of Severity</b>	<b>To be completed by the Investigating Officer in consultation with the Manager of Department affected by the breach and, if appropriate, IT where applicable</b>
<b>Details of the IT systems, equipment, devices, records involved in the security breach:</b>	
<b>Details of information loss:</b>	
What is the nature of the information lost? Is the information unique?	
How much data has been lost?	
If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
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:	



# Choices Academy

<p><b>HIGH RISK</b> personal data  <b>Sensitive</b> personal data (as defined in the Data Protection Act/GDPR) relating to an identifiable individual 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.</p>	
<p>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.</p>	
<p>Personal information relating to vulnerable adults and children.</p>	
<p>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.</p>	
<p>Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.</p>	
<p>Security information that would compromise the safety of individuals if disclosed.</p>	
<p><b>Data Protection Officer and/or Investigating Officer</b> to consider whether it constitutes a reportable data breach.</p>	



# Choices Academy

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