

## DATA PROTECTION POLICY

---

### Introduction

Currency UK Ltd needs to collect and use certain types of information about the Data Subjects who come into contact with it in order to carry on our work. This personal information must be collected and dealt with appropriately– whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this under the Data Protection Act 1998.

The following list below of definitions of the technical terms we have used and is intended to aid understanding of this policy.

**Data Controller** – The person who (either alone or with others) decides what personal information Currency UK Ltd will hold and how it will be held or used.

**Data Protection Act 1998** – The UK legislation that provides a framework for responsible behaviour by those using personal information.

**Data Protection Officer** – The person(s) responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998

**Data Subject/Service User** – The individual whose personal information is being held or processed by Currency UK Ltd (for example: a client, an employee, a supporter)

**‘Explicit’ consent** – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing\* of personal information\* about her/him. Explicit consent is needed for processing sensitive\* data

\* See definition

**Notification** – Notifying the Information Commissioner about the data processing activities of Currency UK Ltd as certain activities may be exempt from notification.

**Information Commissioner** – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

**Processing** – means collecting, amending, handling, storing or disclosing personal information

**Personal Information** – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual employees within Currency UK Ltd.

**Sensitive data** – means data about:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership



- Physical or mental health
- Sexual life
- Criminal record
- Criminal proceedings relating to a data subject's offences

### **Data Controller**

Currency UK Ltd is the Data Controller under the Act, which means that it determines what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

### **Disclosure**

Currency UK Ltd may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows Currency UK Ltd to disclose data (including sensitive data) without the data subject's consent.

These are:

1. Carrying out a legal duty or as authorised by the Secretary of State
2. Protecting vital interests of a Data Subject or other person
3. The Data Subject has already made the information public
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion
6. Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

Currency UK Ltd regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Currency UK Ltd intends to ensure that personal information is treated lawfully and correctly.

To this end, Currency UK Ltd will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998.

Specifically, the Principles require that personal information:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
3. Shall be adequate, relevant and not excessive in relation to those purpose(s)
4. Shall be accurate and, where necessary, kept up to date,
5. Shall not be kept for longer than is necessary
6. Shall be processed in accordance with the rights of data subjects under the

Act,

7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
8. 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 information.

Currency UK Ltd will, through appropriate management, strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information,
- Meet its legal obligations to specify the purposes for which information is used,
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
- Ensure the quality of information used,
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
  - The right to be informed that processing is being undertaken,
  - The right of access to one's personal information
  - The right to prevent processing in certain circumstances and
  - The right to correct, rectify, block or erase information which is regarded as wrong information),
- Take appropriate technical and organisational security measures to safeguard personal information,
- Ensure that personal information is not transferred abroad without suitable safeguards,
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
- Set out clear procedures for responding to requests for information.

## **Data collection**

### **Informed consent**

Informed consent is when

- A Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- and then gives their consent.

Currency UK Ltd will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, Currency UK Ltd will ensure that the Data Subject:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing



- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- Has received sufficient information on why their data is needed and how it will be used

### **Data Storage**

Information and records relating to service users will be stored securely and will only be accessible to authorised staff.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is Currency UK Ltd responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

### **Data access and accuracy**

All Data Subjects have the right to access the information Currency UK Ltd holds about them. Currency UK Ltd will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, Currency UK Ltd will ensure that:

- Everyone processing personal information understands that they are contractually responsible for following good data protection practice,
- Everyone processing personal information is appropriately trained to do so,
- Everyone processing personal information is appropriately supervised,
- Anybody wanting to make enquiries about handling personal information knows what to do,
- It deals promptly and courteously with any enquiries about handling personal information,
- It describes clearly how it handles personal information,
- It will regularly review and audit the ways it holds, manages and uses personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

### **Subject Access Requests:**

An individual is entitled on making a written request to be supplied with a copy of personal information held by Currency UK of which they are the data subject. This is subject to a number of exceptions as prescribed by the Data Protection Act 1998.

Requests for personal information are known as Subject Access Requests. There is an obligation on Currency UK to comply with a Subject Access Request / request made under the Data Protection Act promptly and, in any event, within 40 days of the date of receipt of the request by Currency UK.

### *Making a Subject Access Request:*

Subject Access Requests should be made by the data subject in writing directly to the Currency UK Operations Director. The Applicant may be asked for proof of identity. A Subject Access Request may also be made on behalf of an individual where the individual has expressly consented to the request being made on their behalf. For example, a Solicitor may make a Subject Access Request on behalf of their client. In such cases Currency UK will require a Form of Authority to be signed by the Data Subject consenting to the disclosure of the information.

When requested to provide information requested under the Act all Currency UK management must provide all relevant information held by them in relation to the request.

Currency UK reserves the right to request an individual to narrow the scope of their request. Further, in accordance with Section 8(2) of the Data Protection Act Currency UK reserves the right to refuse to provide the data subject with a copy of the information they hold on that data subject where the supply of a copy of the information is not possible or would involve a disproportionate effort on the part of Currency UK.

### **Third Party Requests**

Personal information relating to staff and students cannot normally be disclosed to an unauthorised third party. These include family members, friends, local authorities, government bodies and the police. There are only certain circumstances when personal information can be given to such third parties and these include:

- prevention or detection of a crime
- apprehension or prosecution of offenders
- prevention of serious harm to a third party
- protection of the vital interests of the data subject, e.g. release of medical data where failure could result in serious harm or death
- ensuring health and safety

Third party requests should be made in writing directly to the Currency UK Operations Director. The College need not respond until it is satisfied as to the identity of the individual and their reasoning behind making the request.

### Summary table of Information Classification and Data Management

Class	Description	Storage	Dissemination and access	Example security Measures	Disposal
Public	Public information on behalf of Currency UK e.g. information on web site	Stored on centrally managed facilities backed up on a 24hr basis	<p>Widely available.</p> <p>Unrestricted dissemination via electronic or hard copy.</p> <p>Dissemination must not violate any applicable laws or regulations. Information should be identifiable as from Currency UK.</p> <p>Permissions to modify limited to authorised persons and procedures in place to ensure that information is kept up to date.</p>	<p>Stored on author's centrally managed filestore.</p> <p>Stored on departmental central filestore share with write permissions restricted to authorised individuals.</p>	<p>Electronic data deleted using normal file deletion processes.</p> <p>Printed material disposed of via 'non-confidential' mechanisms (i.e. does not require shredding.)</p>
Confidential	<p>Information which is sensitive or contains personal information relating to individuals, (e.g. employee information such as payroll, notes relating to disciplinary processes, research data containing personal information or information which is of a high value.)</p> <p>Also personal information relating to our Customers, (e.g. bank details, address, telephone numbers)</p>	Stored on centrally managed facilities backed up on a 24hr basis with access restricted to authorised individuals.	Dissemination strictly limited to authorised personnel only.	<p>Stored on centrally managed filestore with access control mechanisms applied.</p> <p>In exceptional circumstances where information is stored on portable electronic storage devices or media, that storage to be encrypted.</p> <p>Printed copies kept secure, (e.g. in locked filing cabinet with only authorised individuals having access.)</p>	<p>On decommissioning of equipment used to store the data, the storage should be securely wiped to an enhanced standard or even physically destroyed.</p> <p>Printed copies to be shredded.</p>

## **Integrity Review**

Integrity of data will be maintained by asking data subjects at every appropriate opportunity to check the accuracy of their information. The nature of Currency UK business requires data checks to be carried out at least once per year in order to maintain accuracy, relevance and data quality.

Currency UK will take steps to correct data following any notification of inaccuracy by a data subject. If there is disagreement over accuracy and Currency UK has reason to continue to hold data which is regarded as inaccurate by the data subject, the data should carry an indication of that fact.

## **Principles and Practices to ensure compliance with Data Protection and Confidentiality**

1 Data Protection Act 1998 - Principles and Practices to ensure compliance Currency UK will put in place procedures to ensure the eight principles in the DPA 98 are met.

1.1 Personal data shall be processed fairly and lawfully Compliance with Data Protection and Currency UK will be achieved by implementing the following measures:

- Complying with the common law duty of confidentiality; which is that any personal information given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the individual.
- Informing the individual who will be processing their data (usually via an information leaflet)
- Ensuring that certain conditions in Schedules 2 and 3 of the Act are met.
- Informing the individual how the data will be processed. This means fully describing how the data will be used i.e. what will be done to the data; for what purposes it will be used, who it will be passed onto, how it will be processed, stored and destroyed.

1.2 To obtain personal data only for specified and lawful purposes and further process it only in a compatible manner. The following must be adhered to:

- Personal data must only be processed for the purposes for which it was originally obtained.
- Protocols should be in place to ensure that personal data that is passed on is used only for the purposes for which it was originally obtained.

1.3 Personal data must be adequate, relevant and not excessive

This will be achieved by:

- Conducting routine audits as part of good data management practice.



#### 1.4 Personal data must be accurate and up to date.

This will be achieved by:

- Data users recording information accurately and taking reasonable steps to check the accuracy of information they receive from data subjects or anyone else.
- Data users regularly checking all systems to destroy out-of-date information and correcting inaccurate information.

#### 1.5 Personal data must be kept no longer than necessary.

This will be achieved by:

- Adherence to Currency UK Records Management Policy
- Staff working in joint team situations using the maximum retention period.

#### 1.6 Personal data must be processed in accordance with the rights of the individual.

- The Act gives seven rights to individuals, they are a:
- right of subject access (e.g. to see or have a copy of your medical records or staff files)
- right to prevent processing likely to cause damage or distress
- right to prevent processing for the purposes of direct marketing
- rights in relation to automated decision taking
- right to take action for compensation if the individual suffers damage
- right to take action to correct, block, erase or destroy inaccurate data
- right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

### **Currency UK Audit Procedure**

#### *Scope of the audit*

All personal data held in electronic format or contained within a structured manual filing system must be audited.

In particular, but not exclusively, the audit will cover personal data held in the following systems and formats:

- Computer databases;
- Document management systems (including documents stored in standard directory structures provided by such facilities as CFS)
- Individual computer files where appropriate eg. spreadsheets and other such analysis tools, word-processed lists;
- Structured e-mail directories;
- Structured manual filing systems that can be referenced by individual e.g. Student files, staff files, survey data forms, examination scripts, holiday charts/lists, directories, publication lists;
- Web-pages
- Photographs
- Microfiche
- Video/audio recordings
- Tissue samples





Please note that in conducting the audit it will be necessary to meet with all staff within the department to ensure that all processing of personal data is covered.

#### *Frequency of audit*

Departments must conduct an audit on an annual basis. After the initial audit, subsequent audits should require only the amendment of previous audit details. Between each audit any changes in processing (additions, deletions and amendments) must be notified to the Data Protection Officer.

#### *The Audit Process*

For each collection of data an Audit Form must be completed. The form is in two parts. Part A requires the completion of details for notification purposes (and also for assisting in responding to data subject access requests). Part B is a series of questions intended to highlight any areas of non-compliance. A copy of the form is given in Appendix A. Instructions for completing both parts of the form are given below.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.