COURAGE CONSULTANTS UK LIMITED

Data Protection and Privacy Policy

Version 2.0
Date Created 01/07/2021
Most Recent Review Date 19/09/2023
Next Review Date 19/09/2024

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP

COURAGE CONSULTANTS UK LIMITED

Version Control

Document Title	Courage Consultants UK Limited Data Protection and Privacy Policy
Version	Version 2.0
Approved by	Omoruyi Courage Ogbewe
Policy Lead	Omoruyi Courage Ogbewe
Date of Original Approval	01/07/2021
Date of Last Review	19/09/2023
Changes made at the last review	Document Overhaul
Date effective from	19/09/2023
Date of next review	19/09/2024

Contents

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP

COURAGE CONSULTANTS UK LIMITED

1. Introduction and Scope

1.1. Courage Consultants UK Limited needs to collect, store and process personal data about its staff, students, and other individuals it has dealings with, to carry out our functions and activities.

1.2. Courage Consultants UK Limited is committed to a policy of protecting the rights and privacy of individuals, including learners, staff and others, in accordance with the General Data Protection Regulation (GDPR) 2018 2018 and the United Kingdom General Data Protection Regulation (UK GDPR).

1.3. The data controller is; Courage Consultants UK Limited, a company registered in England and Wales with company number 11843588. Our registered office is at:

Courage Consultants UK Limited
Unit 122 , Riverpark Business Center
Riverpark Road
Manchester
M40 2XP

1.4. This Data Protection and Privacy Policy sets out how Courage Consultants UK Limited ("we", "our", "us") handle, uses and protects the personal information of our staff, clients, suppliers, partners, employees, workers and other third parties.

1.5. Courage Consultants UK Limited obtains, uses, stores and otherwise processes personal data relating (but not limited) to potential staff and students (applicants), current staff and students, former staff and students, current and former workers, contractors, website users and contacts, collectively referred to in this policy as data subjects.

1.6. To comply with the law, Courage Consultants UK Limited must ensure that information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

1.7. This policy applies to all individuals about whom Courage Consultants UK Limited hold data (e.g. members of the Board of Management, staff, prospective staff and students.) for processing of personal data carried out for a purpose within Courage Consultants UK Limited, irrespective of whether the data is processed on non-internal equipment or by third parties. More stringent conditions apply to the processing of special category personal data.

1.8. Mandatory training will be provided to staff to assist them in meeting their obligations under this policy. As a matter of good practice, other agencies and individuals working with Courage Consultants UK Limited, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that partners and services who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them. Any individual who does not think they are sufficiently aware of Data Protection Law should contact Data Protection Officer on

courage@courageconsultants.co.uk to arrange additional training. Courage Consultants UK Limited will regularly test our systems and processes to monitor compliance. For Data Protection purposes and compliance matters, please contact courage@courageconsultants.co.uk

1.9. This policy provides a framework for ensuring that Courage Consultants UK Limited meets its obligations under the General Data Protection Regulation (GDPR) and associated data privacy legislation.

1.10. Data protection is about regulating the way that Courage Consultants UK Limited uses and stores information about identifiable people (Personal Data). Please refer to Appendix B for examples of the types of data that can constitute 'Personal Data'.

1.11. It also gives people various rights regarding their data - such as the right to access the personal data that Courage Consultants UK Limited holds on them. We try to avoid using legalese or jargon in this policy; however, certain words and phrases have particular meanings under data protection legislation. Please refer to the Glossary at Appendix A for definitions used in this policy.

1.12. This policy therefore seeks to ensure that we:

1. Are clear about how personal data must be processed and Courage Consultants UK Limited's expectations for all those who process personal data on its behalf;
2. Comply with the data protection law and with good practice;
3. Protect Courage Consultants UK Limited's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights
4. Protect Courage Consultants UK Limited's from risks of personal data breaches and other breaches of data protection law.

1.13. This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject. All staff and others processing personal data on Courage Consultants UK Limited's behalf must read it. A failure to comply with this policy may result in disciplinary action.

1.14. All Managers are responsible for ensuring that all staff within their area of responsibility comply with this policy and should implement appropriate practices, processes, controls and training to ensure that compliance.

1.15. If you are involved in study arrangements with any of Courage Consultants UK Limited Collaborative Partner Institutions, please note that all our partners are also data controllers and are responsible for the same regulations as Courage Consultants UK Limited and must comply with Data Protection Act 2018 and UK GDPR. Please refer to each of our Partner Institutions specifically for further information on their data protection guidelines.

1.16. We may change this notice from time to time by updating it. You should check this notice from time to time to ensure that you are familiar with any changes. For any queries regarding the Data Protection Policy and any issues relating to compliance and data protection matters please contact our Data Protection Officer on courag@courageconsultants.co.uk

2. The Principles of Data Protection

2.1. We adhere to the eight principles relating to Processing of Personal Data set out in Chapter 2 Article 5 UK GDPR. The legislation places a responsibility on every data controller to process any personal data in accordance with this.

2.2. Courage Consultants UK Limited is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below:

2.2.1. Lawfulness, Fairness and Transparency

Courage Consultants UK Limited will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

2.2.2. Purpose Limitation

Personal Data is to be used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes. Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose. Courage Consultants UK Limited will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

2.2.3. Data Minimisation

Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed. Courage Consultants UK Limited will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

2.3.4. Accuracy

Keep personal data accurate and, where necessary, up to date. Courage Consultants UK Limited will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify Courage Consultants UK Limited if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of Courage Consultants UK Limited to ensure that any notification regarding the change is noted and acted on.

2.3.5. Storage Limitation

Only keep personal data for as long as is necessary. Courage Consultants UK Limited undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means Courage Consultants UK Limited will undertake a regular review of the information held and implement a weeding process.

Courage Consultants UK Limited will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

2.3.6. Security, Integrity and Confidentiality

Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data. All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

Courage Consultants UK Limited will ensure that all personal data is accessible only to those who have a valid reason for using it. Courage Consultants UK Limited will have in place appropriate security measures e.g. ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):

- keeping all personal data in a lockable cabinet with key-controlled access.
- password protecting personal data held electronically.
- archiving personal data which are then kept securely (lockable cabinet).
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.
- ensuring that PC screens are not left unattended without a password protected screen-saver being used.

In addition, Courage Consultants UK Limited will put in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed. This policy also applies to staff and students who process personal data 'off-site', e.g. when working at home, and in circumstances additional care must be taken regarding the security of the data

2.3.7. Transfer Limitation

Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Courage Consultants UK Limited will not transfer data to such territories without the explicit consent of the individual. This also applies to publishing information on the internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA - so Courage Consultants UK Limited will always seek the consent of individuals before placing any personal data (including photographs) on its website.

If Courage Consultants UK Limited collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

2.3.8. Data Subject's Rights and Requests

Process personal data in accordance with the rights of the data subject under the legislation.

Individuals have various rights under the legislation including a right to:

- be told the nature of the information Courage Consultants UK Limited holds and any parties to whom this may be disclosed.
- prevent processing likely to cause damage or distress.
- prevent processing for purposes of direct marketing.
- be informed about the mechanics of any automated decision making process that will significantly affect them.
- not have significant decisions that will affect them taken solely by automated process.
- sue for compensation if they suffer damage by any contravention of the legislation.
- take action to rectify, block, erase or destroy inaccurate data.
- request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

Courage Consultants UK Limited will only process personal data in accordance with individuals' rights.

2.4. Courage Consultants UK Limited as Data Controller shall be responsible for and must be able to demonstrate compliance with the data protection principles listed above and will implement appropriate technical and organisational measures to ensure compliance. (Accountability).

2.5. More detailed guidance on how to comply with these principles can be found in the GDPR. Please follow this link to the ICO's website (www.ico.gov.uk)

3. Role and Responsibilities

3.1. Courage Consultants UK Limited is registered with the Information Commissioner's Office as a Data Controller. Details of the School's registration are published on the Information Commissioners website.

3.2. Information Commissioner's Office ("ICO")

3.2.1. ICO is the independent regulatory office in charge of upholding information rights in the interest of the public. The organisation covers the Data Protection Act and advises businesses on how to comply with UK GDPR and therefore requires every data controller who is processing personal information to register with the ICO.

3.3. Courage Consultants UK Limited

3.3.1. As the Data Controller, Courage Consultants UK Limited as executive responsibility for ensuring compliance with data privacy legislation. It is responsible for establishing policies and procedures in order to comply with data protection law.

- establishing and maintaining policies and procedures at a central level to facilitate Courage Consultants UK Limited's compliance with data privacy legislation;
- establishing and maintaining guidance and training materials on data privacy legislation and specific compliance issues;

3.4. Data Protection Officer (DPO)

3.4.1. The DPO is responsible for monitoring internal compliance, advising on Courage Consultants UK Limited's data protection obligations and acting as a point of contact for individuals and the ICO.

3.4.2. The DPO is responsible for:

- advising Courage Consultants UK Limited and its staff of its obligations under GDPR
- monitoring compliance with this Regulation and other relevant data protection law, Courage Consultants UK Limited's policies with respect to this and monitoring training and audit activities relate to GDPR compliance
- to provide advice where requested on Data Protection Impact Assessments (DPIAs)
- to cooperate with and act as the contact point for the Information Commissioner's Office
- the data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.
- supporting privacy by design and privacy impact assessments;
- responding to requests for advice from departments;
- coordinating a company-wide register exercise to capture the full range of processing that is carried out;
- complying with subject access and other rights based requests made by individuals for copies of their personal data;
- investigating and responding to complaints regarding data privacy (including requests to cease the processing of personal data); and
- keeping records of personal data breaches, notifying the ICO of any significant breaches and responding to any requests that it may make for further information.

3.4.3. In fulfilling these responsibilities, the DPO may also involve, and draw on support from, representatives from sections, departments and divisions.

3.4.4. Any issues related to Data Protection and compliance issues, please contact courage@courageconsultants.co.uk

3.5. Heads of department (or equivalent)

3.5.1. Heads of Department are responsible for ensuring that the processing of personal data in their department conforms to the requirements of data privacy legislation and this policy. In particular, they must ensure that:

- new and existing staff, visitors or third parties associated with the Department who are likely to process personal data are aware of their responsibilities under data privacy legislation. This includes drawing the attention of staff to the requirements of this policy, ensuring that staff who have responsibility for handling personal data are provided with adequate training and, where appropriate, ensuring that job descriptions for members of staff or agreements with relevant third parties reference data privacy responsibilities.
- developing and encouraging good information handling practices within their areas of responsibility.
- ensuring that suspected or actual compromises of personal data are reported immediately - ensuring that breaches are dealt with appropriately

- adequate records of processing activities are kept (for example, by undertaking register exercises);
- Ensuring that activities requiring a Data Protection Impact Assessments (DPIA) are referred to the DPO.
- privacy notices are provided where data is collected directly from individuals or where data is used in non-standard ways;
- data sharing is conducted in accordance with Courage Consultants UK Limited's guidance;
- data privacy risks are included in the department's risk management framework and considered by senior management on a regular basis;
- departmental policies and procedures are adopted where appropriate.
- only use personal data in ways people would expect and for the purposes for which it was collected;
- ensuring that their staff have completed all required training in Data Protection.
- use a minimum amount of personal data and only hold it for as long as is strictly necessary;
- keep personal data secure and up-to-date, in accordance with the Courage Consultants UK Limited's Information Security Policy;
- do not disclose personal data to unauthorised persons, whether inside or outside of Courage Consultants UK Limited;
- report promptly any suspected breaches of data privacy legislation, and following any recommended next steps;
- seek advice from the DPO where unsure how to comply with data privacy legislation; and
- promptly respond to any requests from the DPO in connection with subject access and other rights based requests and complaints (and forward any such requests that are received directly to the DPO promptly).

3.6. ICT Department

3.6.1. ICT are responsible for ensuring that advice and guidance on technical specifications and technical security measures are made available to staff such as the Courage Consultants UK Limited ICT Policy.

3.7. Staff

3.7.1. Staff members who process personal data about students, staff, applicants, alumni or any other individual must comply with the requirements of this policy. Staff members must ensure that:

- no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- all personal data is kept securely;
- personal data is kept in accordance with Courage Consultants UK Limited's retention schedule;
- any queries regarding data protection, including subject access requests and complaints, are promptly directed to the DPO;
- any data protection breaches are swiftly brought to the attention of the Data Protection Officer and that they are able to quickly resolve breaches;
- where there is uncertainty around a data protection matter advice is sought from the

Data Protection Officer.

- only use personal data in ways people would expect and for the purposes for which it was collected;
- ensure that they are processing data in line with Courage Consultants UK Limited policies and requirements
- use a minimum amount of personal data and only hold it for as long as is strictly necessary;
- keep personal data up-to-date;
- keep personal data secure, in accordance with Courage Consultants UK Limited's Information Security Policy;
- Completing all required data protection training including refresher training as and when required

3.7.2. Where members of staff are responsible for supervising students doing work which involves the processing of personal information (for example in research projects), they must ensure that those students are aware of the Data Protection principles.

3.7.3. Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Data Protection Officer.

3.8. Contractors, Short-Term and Voluntary Staff

3.8.1. Courage Consultants UK Limited is responsible for the use made of personal data by anyone working on its behalf. Managers who employ contractors, short term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing. In addition, managers should ensure that:

- any personal data collected or processed in the course of work undertaken for Courage Consultants UK Limited is kept securely and confidentially;
- all personal data is returned to Courage Consultants UK Limited on completion of the work, including any copies that may have been made. Alternatively, that the data is securely destroyed and Courage Consultants UK Limited receives notification in this regard from the contractor or short term / voluntary member of staff;
- Courage Consultants UK Limited receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;
- any personal data made available by Courage Consultants UK Limited, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from Courage Consultants UK Limited;
- do not disclose personal data to unauthorised persons, whether inside or outside Courage Consultants UK Limited;
- Completing all required data protection training including refresher training as and when required
- all practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.
- only use personal data in ways people would expect and for the purposes for which it was collected;
- keep personal data up-to-date;
- report promptly any suspected breaches of data privacy legislation, and following any

recommended next steps;
- seek advice from the DPO where they are unsure how to comply with data privacy legislation; and
- promptly respond to any requests from the DPO in connection with subject access and other rights based requests and complaints (and forward any such requests that are received directly to the DPO promptly).

3.9. Third-Party Data Processors

3.9.1. Where external companies are used to process personal data on behalf of Courage Consultants UK Limited, responsibility for the security and appropriate use of that data remains with Courage Consultants UK Limited

3.9.2. Where a third-party data processor is used:

- a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
- reasonable steps must be taken that such security measures are in place;
- a written contract establishing what personal data will be processed and for what purpose must be set out;
- a data processing agreement, available from the DPO, must be signed by both parties.
- use a minimum amount of personal data and only hold it for as long as is strictly necessary;
- keep personal data up-to-date;
- keep personal data secure, in accordance with Courage Consultants UK Limited's Information Security Policy;
- do not disclose personal data to unauthorised persons, whether inside or outsideof Courage Consultants UK Limited;
- complete relevant training as required;
- report promptly any suspected breaches of data privacy legislation, and following any recommended next steps;
- seek advice from the DPO where they are unsure how to comply with data privacy legislation; and
- promptly respond to any requests from the DPO in connection with subject access and other rights based requests and complaints (and forward any such requests that are received directly to the DPO promptly).

3.9.3. For further guidance about the use of third-party data processors please contact the DPO.

3.10. Students

3.10.1. Students are responsible for:

- familiarising themselves with the Privacy Notice provided when they register with Cou;
- ensuring that their personal data provided to Courage Consultants UK Limited is accurate and up to date.
- only use personal data in ways people would expect and for the purposes for which it was collected;
- use a minimum amount of personal data and only hold it for as long as is strictly necessary;
- keep personal data secure, in accordance with the Courage Consultants UK Limited's

Information Security Policy;

- do not disclose personal data to unauthorised persons, whether inside or outside Courage Consultants UK Limited;
- report promptly any suspected breaches of data privacy legislation, and following any recommended next steps;
- seek advice from the DPO where they are unsure how to comply with data privacy legislation; and
- promptly respond to any requests from the DPO in connection with subject access and other rights based requests and complaints (and forward any such requests that are received directly to the DPO promptly).

3.11. Any issues related to Data Protection and compliance issues, please contact courage@courageconsultants.co.uk

4. Data Subjects' Rights

4.1. Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

1. where the legal basis of our processing is Consent, to withdraw that Consent at any time;
2. to ask for access to the personal data that we hold (see below);
3. to prevent our use of the personal data for direct marketing purposes
4. to object to our processing of personal data in limited circumstances
5. to ask us to erase personal data without delay:
   - if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
   - if the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data;
   - if the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest;
   - if the data subject has objected to our processing for direct marketing purposes;
   - if the processing is unlawful.
6. to ask us to rectify inaccurate data or to complete incomplete data;
7. to restrict processing in specific circumstances e.g. where there is a complaint about accuracy;
8. to ask us for a copy of the safeguards under which personal data is transferred outside of the EU;
9. the right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with Courage Consultants UK Limited; it is based on the data subject's explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards;
10. to prevent processing that is likely to cause damage or distress to the data subject or anyone else;
11. to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
12. to make a complaint to the ICO; and
13. in limited circumstances, receive or ask for their personal data to be transferred to a third party (e.g. another institution to which a student is transferring) in a structured,

commonly used and machine readable format.

4.2. You must verify the identity of an individual requesting data under any of the rights listed

4.3. Requests (including for data subject access – see below) must be complied with, usually within one month of receipt. You must immediately forward any Data Subject Access Request you receive to the DPO at courage@courageconsultants.co.uk. A charge can be made for dealing with requests relating to these rights only if the request is excessive or burdensome.

5. Your Obligations

5.1. Article 6 UK GDPR sets out the Lawfulness of processing: Personal Data must be processed fairly, lawfully and transparently. What does this mean in practice?

a) "Processing" covers virtually everything which is done in relation to Personal Data, including using, disclosing, copying and storing Personal Data.
b) People must be told what data is collected about them, what it is used for, and who it might be shared with, unless it is obvious. They must also be given other information, such as, what rights they have in their information, how long we keep it for and about their right to complain to the Information Commissioner's Office ("ICO").

5.2. This information is often provided in a document known as a Transparency Notice. Copies of Courage Consultants UK Limited Transparency Notices can be obtained from the Data Protection Officer.

5.3. You must only process Personal Data for the following purposes:

a) as set out in the applicable Transparency Notice
b) protecting and promoting Courage Consultants UK Limited legitimate interests and objectives and
c) to fulfil the Courage Consultants UK Limited contractual and other legal obligations.

5.4. Use of Personal Data- If you want to do something with Personal Data that is not on the above list, you must speak to Data Protection Officer (DPO). This is to make sure that Courage Consultants UK Limited has a lawful reason for using the Personal Data. If you are using Personal Data in a way which you think an individual might think is unfair please speak to the Data Protection Officer (DPO).

6. Requests for Personal Data (Subject Access Requests)

6.1. The Data Protection Act 1998 gives data subjects the right to receive a copy of their personal information which is held by Courage Consultants UK Limited. Under this right people are entitled to request a copy of the Personal Data which Courage Consultants UK Limited holds about them and to certain supplemental information.

6.2. Form of request: Subject Access Requests do not have to be labelled as such and do not even have to mention data protection. For example, an email which simply states "Please send me copies of all emails you hold about me" is a valid Subject Access Request. You must always immediately let Courage Consultants UK Limited DPO know when you receive any such requests.

6.3. Please see APPENDIX D for an example of a Subject Access Request. Please note, the subject access request image was obtained from the ICO website.

6.4. Receiving a Subject Access Request is a serious matter for Courage Consultants UK Limited and involves complex legal rights. Staff must never respond to a subject access request themselves unless authorised to do so.

6.5. You should not alter, conceal, block or destroy personal data once a request for access has been made. You should contact the DPO before any changes are made to personal data which is the subject of an access request.

6.6. Disclosure: When a Subject Access Request is made, Courage Consultants UK Limited must disclose all of that person's Personal Data to them which falls within the scope of the request - there are only very limited exceptions. There is no exemption for embarrassing information - so think carefully when writing letters and emails as they could be disclosed following a Subject Access Request. However, this should not deter you from recording and passing on information where this is appropriate to fulfil your professional duties, particularly in relation to money laundering or fraud prevention.

6.7. Further guidance on making a 'subject access request' and the process can be found under Courage Consultants UK Limited Data Subject Access Request Policy

6.8. Please note any access request will be subject to a fee (currently £10) and we will require identification to verify your identity.

6.9. We will not allow third parties to persuade us into disclosing personal data without proper authorisation. For example, students' parents do not have an automatic right to gain access to their child's data.

6.10. Contact us via

6.10.1. writing to us at:

Courage Consultants UK Limited
Unit 122, Riverpark business Centre
Riverpark Road
Manchester
M40 2XP

Marked for the attention of OGBEWE, OMORUYI COURAGE

6.10.2. by telephoning:

01612312038

asking to speak to OGBEWE, OMORUYI COURAGE.

6.11. If your enquiry is in relation to accessing your personal information please also state; Subject Access Request for our convenience.

7. Transfer outside the EU/EEA

7.1. The UK has incorporated the GDPR into the withdrawal bill and pending an adequacy decision, the EU-UK Trade and Cooperation Agreement contains a bridging mechanism that allows the continued free flow of personal data from the EU/EEA to the UK until adequacy decisions come into effect, for up to six months. The UK GDPR requires Data Controllers to ensure that any Personal Data sent to any country outside the EU/EAA is afforded the same level of protection as in the EU.

7.2. Transfers outside the EU/EAA are only permitted in the following situations:

- The European Commission has issued a decision confirming the country receiving the Personal Data is provides an adequate level of protection.
- Appropriate safeguards are in place such as binding corporate rules or standard contractual clauses.
- The data subject has provided explicit consent to the proposed transfer having been informed of all the risks.

7.3. The transfer is necessary for one of the reasons set out in the UK GDPR including:

- The performance of a contract.
- Reasons of public interest.
- For the establishment or defence of legal claims.
- In the Vital Interests of a Data Subject.

7.4. Where transfers are being made out of the EU/EEA, advice should be sought from Courage Consultants UK Limited Academic Standards and Quality Office (ASQO). For more information on transfers outside the EU/EEA, please visit ICO website.

8. Consent

8.1. Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner. Consent is especially important when Courage Consultants UK Limited is processing any sensitive data, as defined by the legislation.

8.2. Courage Consultants UK Limited understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via the enrolment form) whilst being of a sound mind and without having any undue influence exerted upon them.

8.3. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

8.4. Consent is required for certain mail-outs and marketing by electronic means, please check with the DPO before sending mail-outs to client

9. Record Keeping

9.1. The GDPR requires us to keep full and accurate records of all our data processing activities. You must keep and maintain accurate corporate records reflecting our processing, including records of data subjects' Consents and procedures for obtaining Consents, where Consent is the legal basis of processing.

9.2. These records should include, at a minimum, the name and contact details of Courage Consultants UK Limited as Data Controller and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

9.3. Records of personal data breaches must also be kept, setting out:

1. the facts surrounding the breach
2. its effects; and
3. the remedial action taken

10. Breaches of Data Privacy Legislation

10.1. Courage Consultants UK Limited will investigate incidents involving a possible breach of data privacy legislation in order to ensure that, where necessary, appropriate action is taken to mitigate the consequences and prevent a repetition of similar incidents in future.

10.2. Depending on the nature and severity of the incident, it may also be necessary to notify the individuals affected and/or the ICO.

10.3. A breach will occur where, for example, personal data is disclosed or made available to unauthorised persons or personal data is used in a way that the individual does not expect.

10.4. Incidents involving failures of IT systems or processes must be reported to the DPO within 4 working hours of discovery. All other incidents must be reported directly to the DPO at the earliest possible opportunity.

11. Compliance

11.1. Courage Consultants UK Limited regards any breach of data privacy legislation, this policy or any other policy and/or training introduced by Courage Consultants UK Limited from time to time to comply with data privacy legislation as a serious matter, which may result in disciplinary action.

11.2. Depending on the nature of the breach, an individual may also find that they are personally liable (for example, it can be a criminal offence for a member of Courage Consultants UK Limited to disclose personal information unlawfully).

12. Reporting a Personal Data Breach

12.1. The GDPR requires that we report to the Information Commissioner's Office (ICO) any personal data breach where there is a risk to the rights and freedoms of the data subject.

12.2. Where the Personal data breach results in a high risk to the data subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly.

12.3. In the latter circumstances, a public communication must be made or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.

12.4. We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or the ICO where we are legally required to do so.

12.5. If you know or suspect that a personal data breach has occurred, you should immediately contact the DPO at Courage@courageconsultants.co.uk and follow the instructions in the personal data breach procedure.

12.6. You must retain all evidence relating to personal data breaches in particular to enable Courage Consultants UK Limited to maintain a record of such breaches, as required by the GDPR.

12.7. Courage Consultants UK Limited takes compliance with the Data Protection policy very seriously, therefore a breach of this policy may be treated as misconduct and could result in disciplinary action and in serious cases, may lead to dismissal. If staff or students are found to be in breach of this policy, Courage Consultants UK Limited has the authority to revoke your access to the Schools systems, whether through a device or otherwise. Failure to comply with the policy can lead to:

- Damage and distress being caused to those who entrust us to look after their personal data, risk of fraud or misuse of compromised personal data, a loss of trust and a breakdown in relationships with the School.
- Damage to Courage Consultants UK Limited reputation and its relationship with its stakeholders (including research funders and prospective students and collaborators).

13. Personal Data at Work

13.1. In order for you to do your job, you will need to collect, use and create Personal Data. Virtually anything that relates to a living person will include Personal Data. Examples of places where Personal Data might be found are:

a) on a computer database
b) in a file, such as a personnel or client record
c) in a register or contract of employment
d) letters, attendance notes, meeting minutes and other documents or written records

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP

e) health records
f) email correspondence
g) work mobile telephones
h) work tablets

13.2. Categories of Critical Courage Consultants UK Limited Personal Data:

13.3. The following categories are referred to as Critical Courage Consultants UK Limited Personal Data in this policy. You must be particularly careful when dealing with Critical Courage Consultants UK Limited Personal Data which falls into any of the categories below:

a) physical or mental health or condition
b) racial or ethnic origin
c) religious beliefs or other beliefs of a similar nature
d) information relating to actual or alleged criminal activity; and
e) genetic or biometric information

13.4. If you have any questions about your processing of these categories of Critical Courage Consultants UK Limited Personal Data please speak to Courage Consultants UK Limited Data Protection Officer who will be happy to assist you. Any issues relating to compliance please use courage@courageconsultants.co.uk.

14. Processing Personal Data: Responsibilities of Staff

14.1. Personal Data must only be processed for limited purposes and in an appropriate way. What does this mean in practice?

14.2. For example, if employees are told that they will be photographed for Courage Consultants UK Limited website or intranet, you should not use those photographs for another purpose (e.g., Courage Consultants UK Limited marketing material or social media accounts).

14.3. When you are designing a new process or procedure you must take account of the Privacy by Design requirements which include undertaking an appropriate Data Protection Impact Assessment. When you are planning your changes, please speak to Courage Consultants UK Limited DPO for advice and assistance.

14.4. Personal Data held must be adequate and relevant for the purpose. What does this mean in practice?

14.5. This means not making decisions based on incomplete data. For example, when undertaking an employee's performance review, you must make sure you are using all the relevant and most up to date information about the employee.

14.6. Personal Data must not be excessive or unnecessary. What does this mean in practice?

14.7. Personal Data must not be processed in a way that is excessive or unnecessary. For example, you should only collect information about an employee's family when it is necessary in relation to work, such as to ensure Courage Consultants UK Limited is aware of an employee's childcare arrangements to assist with flexible working.

14.8. Personal Data that you hold must be accurate. What does this mean in practice?

14.9. You must ensure that Personal Data is complete and kept up to date. For example, if a students, staffs, or client's contact details have changed, you should update Courage Consultants UK Limited information management system.

14.10. Personal Data must not be kept longer than necessary. What does this this mean in practice?

14.11. Courage Consultants UK Limited holds different types of data for different amounts of time. This applies to both paper and electronic documents. You must be particularly careful when you are deleting data. Please speak with Courage Consultants UK Limited DPO for guidance on the retention periods and secure deletion.

14.12. Personal Data must be kept secure. You must comply with the following Courage Consultants UK Limited policies and guidance relating to the handling of Personal Data, which can be found in the Staff Handbook:

a) CCTV & security
b) Monitoring
c) Email and internet use
d) Social media
e) Anti-corruption & bribery; and
f) Screening

14.13. Personal Data must not be transferred outside the EEA without adequate protection. What does this mean in practice?

14.14. If you need to transfer personal data outside the EEA please contact Courage Consultants UK Limited DPO. For example, if you are arranging a Courage Consultants UK Limited trip to a country outside the EEA or working with a client based outside the EEA.

15. Sharing Personal Data Outside of Courage Consultants UK Limited – Dos and Don'ts

15.1. Please review the following dos and don'ts:

15.2. DO share Personal Data strictly on a need-to-know basis - think about why it is necessary to share data outside Courage Consultants UK Limited - if in doubt - always ask your line manager.

15.3. DO encrypt emails which contain Critical Courage Consultants UK Limited Personal Data. For example, encryption should be used when sending details of an employee's ill health to external advisers or insurers; or payroll details which are likely to contain several pieces of Critical Courage Consultants UK Limited Personal Data including details of trade union membership to the payroll provider.

15.4. DO make sure that you have permission from your line manager or Courage Consultants UK Limited DPO to share Personal Data on Courage Consultants UK Limited website.

15.5. DO be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. You should seek advice from Courage Consultants UK Limited DPO where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g., if a request has come from an existing client but using a different email address).

15.6. DO be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Don't reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise. Report all concerns about phishing to the IT department.

15.7. DO NOT disclose Personal Data to the Police or other statutory agencies such as HMRC or a Local Authority without permission from Courage Consultants UK Limited DPO.

15.8. DO NOT disclose Personal Data to contractors without permission from Courage Consultants UK Limited DPO. This includes, for example, sharing Personal Data with an external marketing team to carry out a marketing campaign. For more examples on Staff Do's and Don'ts please see APPENDIX C.

16. Processing Personal Data: Responsibilities of Students

16.1. This policy applies to students where they are collecting personal information on behalf of Courage Consultants UK Limited, for example conducting research and collecting personal data as part of their role as Student Representative. In connection with students' academic studies/research if required or necessary, all Courage Consultants UK Limited students have the following responsibilities:

- To notify an appropriate member of staff, usually their tutor, if they intend to process information about identifiable individuals as part of their academic studies/research.
- To only process Personal Data for use in academic studies/research which has been expressly authorised by a member of staff.
- To comply with any regulations or requirements implemented by Courage Consultants UK Limited or by a member of Courage Consultants UK Limited staff in order to facilitate compliance with Data Protection Law; and
- To have reference and to adhere to Courage Consultants UK Limited Data Protection Policy, Procedures and Guidelines at all times.

16.2. In relation to any activities not specifically authorised by Courage Consultants UK Limited, students processing Personal Data are responsible for their own compliance with Data Protection Law.

17. Sharing Personal Data with Courage Consultants UK Limited

17.1. This section applies when Personal Data is shared within Courage Consultants UK Limited. Personal Data must only be shared within Courage Consultants UK Limited on a "need to know" basis.

17.2. Client files should be locked down to the Staff who need to access the information for business purposes and wider access granted only to persons with appropriate authority. If you are unsure whether a person has appropriate authority speak to Courage Consultants UK Limited DPO.

17.3. Examples of internal sharing which are likely to comply with the UK GDPR:

a) liaising with Human Resources Management with CEO and Senior Managers in respect of employees' pay reviews.

17.4. Examples of internal sharing which are unlikely to comply with the UK GDPR:

b) recording an interview or telephone call without the other person knowing, leaving handover notes on a colleague's desk while they are away, using your personal mobile device without Courage Consultants UK Limited consent.

18. Individuals' Rights in their Personal Data

18.1. The UK GDPR and DPA 2018 provides you with Individual's rights: People have various rights to their information. You must be able to recognise when someone is exercising their rights so that you can refer the matter to Courage Consultants UK Limited DPO. Please let Courage Consultants UK Limited DPO know if anyone (either for themselves or on behalf of another person, such as a solicitor):

- The right of access/to be informed-wants to know what information Courage Consultants UK Limited holds about them.
- The right to withdraw -asks to withdraw any consent that they have given to use their information.
- The right to erasure-wants Courage Consultants UK Limited to delete any information.
- The right to rectification-asks Courage Consultants UK Limited to correct or change information (unless this is a routine updating of information such as contact details, which falls within your role and authorised access).
- The right to data portability-asks for electronic information which they provided to Courage Consultants UK Limited to be transferred back to them or to another organisation.
- The right to restrict processing- wants Courage Consultants UK Limited to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as Courage Consultants UK Limited; or
- The right to object- objects to how Courage Consultants UK Limited is using their information or wants the Courage Consultants UK Limited to stop using their information in a particular way, for example, if they are not happy that information has been shared with a third party.

18.2. For more information on the above UK GDPR rights, please revert to the ICO website.

19. Criminal Offence

19.1. A member of staff or student who deliberately or recklessly misuses or discloses Personal Data held by Courage Consultants UK Limited without proper authority, could lead to a criminal offence. Failure to comply with the policy carries the risk of significant civil and criminal sanctions for the individual and the school, which can lead to:

- Significant legal and financial consequences. Monetary penalties of the Information Commissioners Office can reach up to 20 million euros or 4% of turnover.
- Individual civil action for breaches of data protection can also be taken by individuals or third-party organisations where there is a failure to meet contractual obligations to hold data securely.

20. Alternative Format

20.1. This policy can be provided in alternative formats (including large print, audio and electronic) upon request. For further information, or to make a request, please contact: courage@courageconsultants.co.uk

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP

Appendix A – Glossary

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to Courage Consultants UK Limited Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

United Kingdom General Data Protection Regulation (UK GDPR): The United Kingdom General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Data Protection Impact Assessments (DPIA): A Data Protection Impact Assessment (DPIA) is a process to help companies identify and minimise the data protection risks of a project. This is carried out for processing that is likely to result in a high risk to individuals in regard to their personal data.

Information Commissioner's Office ("ICO"): ICO is the independent regulatory office in charge of upholding information rights in the interest of the public. The organisation covers the Data Protection Act and advises businesses on how to comply with UK GDPR and therefore requires every data controller who is processing personal information to register with the ICO.

Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with UKGDPR.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data

including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

Staff: all employees, workers, contractors, agency workers, consultants, directors, members, agency staff, temporary staff, work experience and volunteers and others.

Student: a person who is studying at Courage Consultants UK Limited or other place of higher education to attain a particular qualification to help enter a particular profession.

Transparency Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when Courage Consultants UK Limited collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee Transparency Notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP

COURAGE CONSULTANTS UK LIMITED

Appendix B – Personal Data

The following are examples of the types of data that can constitute 'Personal data':

- Name
- Data of Birth/Age
- Postal Address(es) (to include postcodes)
- Contact telephone(s)
- Email address(es)
- Unique Identifiers (to include Student ID numbers, Staff ID numbers, Passport numbers, NHS numbers, National Insurance numbers, Unique applicant ID numbers, vehicle reg, driving licence numbers)
- Images of individuals, including CCTV, photos.
- Location Data (to include any GPS tracking data)
- Online Identifiers (to include IP address data)
- Economic/financial data (relating to an identifiable individual)
- Educational records including but not limited to records held by Courage Consultants UK Limited /other education providers.
- Counselling records
- Pastoral records, including Extenuating Circumstances Forms
- Disciplinary records/Training records
- Employment records to include CV's, references.
- Nationality/Domicile
- Ethnicity
- Mental Health (status, medical records conditions, to include disability)
- Physical Health (status, medical records conditions, to include disability)
- Dietary requirements
- Sexual Orientation/Sexual life
- Genetic Data (to include DNA data)
- Biometric data (such as facial image or fingerprint data)
- Political opinions/Trade Union membership
- Religious or philosophical beliefs
- Criminal Convictions and offences (to include alleged offences and convictions)

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP

Appendix C – Staff Guide on Sharing Personal Data: Dos and Don'ts

All Courage Consultants UK Limited staff must ensure that the requirements of the UK Data Protection Act 2018 are observed at all times. Guidance is given below concerning what you should do and what you should not do in this respect. Please read this guidance carefully and try to ensure you adhere to guidance at all times. If you have any questions or areas for clarification please contact Courage Consultants UK Limited Academic Standards and Quality Office (ASQO), courage@courageconsultants.co.uk, in the first instance. A folder on SharePoint 'Courage Consultants UK Limited Internal Data Protection Policies and Procedures' has been created for you to access. In the first instance this guidance is available there.

DO's

DO share Personal Data strictly on a need-to-know basis - think about why it is necessary to share data outside of Courage Consultants UK Limited - if in doubt - always ask your line manager.

DO encrypt emails which contain Critical Courage Consultants UK Limited Personal Data. For example, encryption should be used when sending details of an employee's ill health to external advisers or insurers; or payroll details which are likely to contain several pieces of Critical Courage Consultants UK Limited Personal Data including details of trade union membership to the payroll provider.

DO make sure that you have permission from your line manager or Courage Consultants UK Limited DPO to share Personal Data on Courage Consultants UK Limited website.

DO be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. You should seek advice from Courage Consultants UK Limited DPO where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g., if a request has come from an existing client but using a different email address).

DO be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords.

DO shred personal data if in paper form and arrange certified confidential waste disposal for large amounts of personal data as and when approved and required by Courage Consultants UK Limited.

DO keep your username and passwords secure and do not share these amongst colleagues

DO report any data breaches immediately and undertake regular training on Data Protection and UK GDPR

DO verify an individual before handing over personal data, whether its by phone, email or face to face.

DO be vigilant with emails and attachments

DO familiarise yourself with all Courage Consultants UK Limited policies and procedures

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP

DO log out when not using digital services especially Courage Consultants UK Limited internal emails and software such as Moodle, teams, Microsoft Outlook.

DO audit the data you are using on a day-to-day basis within the scope of UK GDPR.

DONT'S

DO NOT leave any personal information lying around at home or in the office

DO NOT give your username or password to anyone

DO NOT dispose of personal data in regular bins or recycling if it has not been shredded or destroyed

DO NOT open emails or attachments from unknown sources

DO NOT duplicate personal data unnecessarily e.g. printing it out

DO NOT download Courage Consultants UK Limited data onto personal devices unless authorised to do so

DO NOT leave your computer logged in if you can access personal data from it i.e. student information or sensitive information

DO NOT store your passwords in browsers

DO NOT log into public wi-fi or unsecured networks whilst working with personal data

DO NOT provide access to personal data unless it is necessary and lawful

DO NOT disclose Personal Data to the Police or other statutory agencies such as HMRC or a Local Authority without permission from Courage Consultants UK Limited DPO.

DO NOT disclose Personal Data to contractors without permission from Courage Consultants UK Limited DPO This includes, for example, sharing Personal Data with an external marketing team to carry out a marketing campaign.

DO NOT put actual student names in emails, instead use code such as Student A, Student B, Student C so on and so forth.

DO NOT circulate emails to others with emails addresses on, especially if private email addresses of staff or student or external to Courage Consultants UK Limited.

DO NOT keep inaccurate data as this is a breach of data protection legislation

DO NOT assume that data protection doesn't matter – IT DOES

DO NOT reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise. Report all concerns about phishing to the IT department.

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP

COURAGE CONSULTANTS UK LIMITED

Appendix D – Example Subject Access Request

[Name and address of the organisation]

[Your name and full postal address]

[Your contact number]

[Your email address]

[The date]

Dear Sir or Madam

Subject Access Request

[Include your full name and other relevant details to help identify you].

Please supply the personal data you hold about me, which I am entitled to receive under data protection law, held in:

[Give specific details of where to search for the personal data you want, for example:

- My personal file;
- Emails between 'Person A' and 'Person B' (from 1 June 2017 to 1 Sept 2017);
- My medical records (between 2014 and 2017) held by 'Dr C' at 'Hospital D';
- The CCTV camera situated at ('location E') on 23 May 2017 between 11am and 5pm; and
- Financial statements (between 2013 and 2017) held in account number xx-xx-xx.]

If you need any more information, please let me know as soon as possible.

[If relevant, state whether you would prefer to receive the data in a particular electronic format, or printed out].

It may be helpful for you to know that data protection law requires you to respond to a request for personal data within one calendar month.

If you do not normally deal with these requests, please pass this letter to your data protection officer or relevant staff member.

If you need advice on dealing with this request, the Information Commissioner's Office can assist you. Its website is ico.org.uk, or it can be contacted on 0303 123 1113.

Yours faithfully

[Signature]

Please note, the above subject access request example was obtained from the ICO website.

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP