Data Protection Policy	**Date updated:** Jan 17 **Approved by:** BOARD **Responsible for:** D of FCS **Review date:** Jan 18

1 About the Data Protection Policy

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of the organisation's activities it will collect, store and process personal data about customers, suppliers and other third parties. It is recognised that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

All data users are obliged to comply with this policy when processing personal data on the organisation's behalf, which includes all employees and secondees. Consultants are obliged to adhere to this policy as part of their service agreement; contracting Managers are responsible for ensuring consultants' adherence. Any breach of this policy may result in disciplinary action.

1.2 The Director of Finance and Corporate Services is responsible for this policy. Please contact the Director of Finance and Corporate Services in the first instance for further information.

2 Policy Statement

2.1 The organisation aims to fulfil its obligations under the Data Protection Act 1998 (DPA) to the fullest extent. The DPA sets out 8 principles which should be followed by those who process data; it also gives rights to those whose data is being processed. The organisation endorses fully, and adheres to, the eight principles of data protection, as set out in the DPA (see section 5 below for further guidance on the eight principles).

This policy, and any other documents referred to in it, sets out the basis on which the organisation will process any personal data it collects from data subjects, or that is provided to it by data subjects or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy sets out rules on data protection and the legal conditions that must be satisfied when the organisation obtains, handles, processes, transfers and stores personal data.

The Director of Finance and Corporate Services is the organisation's **'designated data controller'** and is responsible for ensuring compliance with the Act and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Director of Finance and Corporate Services.

Note: For quick reference purposes you will find data protection dos and don'ts list at section 13 below. However, that list is not intended to summarise this policy and as such it should be read in addition to, and not instead of, this policy.

3 Information Commissioner

3.1 The Information Commissioner is the independent regulator charged with policing and enforcing data protection legislation in the UK and with promoting good practice for compliance purposes.

The web site of the Information Commissioner's Office (www.ico.org.uk) contains a wide range of useful information and guidance, both technical (legal) and practical, about the legislative regime and what it requires.

4 When Does Data Protection Legislation Apply?

4.1 The DPA aims to ensure fairness, transparency and accountability in the "processing" of "personal data". It does so by requiring organisations which are "data controllers" to comply in their processing of personal data with eight data protection principles (the 8 principles are outlined below at section 5).

A "**data controller**" is any legal entity which determines the purposes for which and the manner in which personal data are held and used. The organisation is a data controller in respect of the vast majority of the personal data which it holds, whether about customers, staff, suppliers or anyone else.

"**Personal data**" is (broadly) any information about a living individual which the organisation holds electronically or in hard copy. For example, personal data includes information about any one or more living individuals which the organisation holds:

- in emails;
- in any other correspondence and provision of services such as Moodle, in each case regardless of whether the organisation drafted it, and whether in electronic form or hard copy;
- in the central marketing database and any other electronic or hard copy database or other collection of contact information, whether about customers, contacts, suppliers or otherwise;
- in the form of an audio or audio visual recording including, for example, as part of recorded dictation or in a voicemail message; and
- in files and records held by the HR department, whether in electronic form or hard copy.

One individual's opinion about another individual is personal data about both of them. Information about any legal person other than a living individual e.g. about a company, a partnership or a public authority, is not personal data. However, information about any of the individuals who work for that entity e.g. employees, contractors etc. is personal data.

"**Sensitive Personal Data**" includes information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission or alleged commission by an individual of any offence or any related proceedings or sentence. The DPA imposes certain additional requirements in respect of the processing of sensitive personal data in order to ensure that it is appropriately safeguarded. Members of staff should therefore always take particular care when dealing with sensitive personal data.

"**Processing**" means holding or otherwise accessing or using personal data in any manner whatsoever; even simply reading it or telling someone about it. Essentially anything which staff do with personal data in the course of their work - including obtaining it, holding it, disclosing it, using it and erasing/destroying it - is likely to amount to processing.

5 DPA Principles

5.1 As outlined above, there are eight data protection principles:

1. **Fair and lawful processing** – personal data is processed fairly and lawfully, an essential prerequisite of which is that all processing can be justified on the basis of at least one from a list of conditions (plus one from a supplemental list, where sensitive personal data is involved)
2. **Limited, specified purposes** – personal data is obtained for one or more specified and lawful purposes and is not further processed in a manner incompatible with that purpose or those purposes
3. **Relevancy and sufficiency** – personal data is adequate, relevant and not excessive in relation to the purpose or purposes for which it is being used
4. **Accuracy** – personal data is accurate and, where necessary, up-to-date
5. **Keep only for so long as required** – personal data is not kept longer than is necessary for the purpose or purposes for which it is being held
6. **Individual rights** – personal data is processed in accordance with the rights of the individual to whom it relates
7. **Security** – appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data
8. **Transfer only to countries where there is adequate protection** – personal data is not transferred outside the European Economic Area unless to a jurisdiction that ensures an adequate level of protection for the rights and freedoms of the individuals to whom it relates.

6 Data Security

6.1 Members of staff are responsible for ensuring that:

- any personal data they hold is kept securely and in accordance with the terms of the organisation's Personal Information Security Policy;
- personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party;
- they comply with this Data Protection Policy.

It should be noted that any unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, the information must be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe. For further information on data and information security, please read our Personal Information Security Policy.

Data should be held and disposed of in accordance with the terms of the organisation's Personal Information and Security Policy and our Document Retention and Destruction Policy.

7 Subject Consent

7.1 In many cases, the organisation can only process personal data with the consent of the individual. If the data being processed is Sensitive Personal Data express consent must be obtained when the data is collected.

8 Staff members Personal Information

8.1 Members of staff are responsible for:

- checking that any information they provide to the organisation in connection with their employment, secondment or consultancy services is accurate and up to date
- informing the organisation of any changes to their personal information, for example changes of address, either at the time of appointment or thereafter.

Please note that the organisation cannot be held responsible for any errors unless members of staff have informed the relevant member of staff of such changes.

9 Transferring Personal Data (to a country outside the EEA)

9.1 The organisation may transfer any personal data it holds to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- the country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- the data subject has given his consent.
- the transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
- the transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
- the transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements in clause 6 above, personal data the organisation holds may also be processed by staff operating outside the EEA who work for the organisation or for one of its suppliers. That staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

10 Disclosure and Sharing of Personal Information

10.1 The organisation may disclose personal data it holds to third parties:

- in the event that the organisation sells or buys any business or assets, in which case it may disclose personal data it holds to the prospective seller or buyer of such business or assets
- if all or substantially all, of the organisation's assets are acquired by a third party, in which case personal data it holds will be one of the transferred assets
- if the organisation is under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect its rights, property, or safety of its employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

The organisation may also share personal data it holds with selected third parties.

11 Subject Access Requests

11.1 <u>General</u>
Data subjects must make a formal request for information the organisation holds about them under the DPA. Such requests require the organisation to respond to requests for access to

personal data within 40 days. Details of an employee's personal data are therefore, available upon request in accordance with the principles of the DPA.

11.2 Access to Data

Members of staff are allowed to have access to any personal data the organisation hold about them. The DPA gives data subjects the right to have access to their personal data at reasonable intervals. Should a member of staff request access to their personal information at any other time, the request must be addressed to the Director of Finance. The request will be judged in the light of the nature of the personal data and the frequency with which they are updated. The member of staff will then be informed whether or not the request is to be granted. If it is, the information will be provided within 40 days of the date of the request.

In the event of a disagreement between a member of staff and the organisation regarding personal data, the matter should be taken up under the grievance procedure.

Where staff members make additional requests for access to their personal data which are granted, a fee of £10 will be charged which must be paid to the Director of Finance and Corporate Services before a copy of the personal data will be given.

11.3 Secondees

Secondees should contact their employer for guidance where there is a disagreement relating to personal data.

Third Parties

Third parties must make access requests in writing. Any member of staff who receives a written request should forward it to the Director of Finance and Corporate Services immediately.

When receiving telephone enquiries, the organisation will only disclose personal data it holds on its systems when the callers identity has been checked to ensure they are entitled to the data.

The organisation may suggest that a caller put their request in writing if their identity cannot be verified or checked.

All members of staff will refer a request to the Director of Finance and Corporate Services for assistance in difficult situations (members of staff should not be bullied into disclosing personal information).

12 Policy Breaches

12.1 If a member of staff thinks they may have breached this policy, they should speak to the Director of Finance and Corporate Services immediately.

Quick action can be crucial in mitigating the negative effects of a breach, in particular where data security is concerned; it is therefore vital that members of staff raise the issue immediately in accordance with this policy.

It should be noted that failure to comply with this policy will constitute a disciplinary offence.

13 Data Protection Dos and Don'ts

13.1 Do

- Do "think data protection". Members of staff should stop to think about whether what they are proposing to do works from a data protection compliance perspective.
- Do remember the two driving principles behind data protection:
    - fairness
    - transparency
- Do think very carefully before doing anything with sensitive personal data.
- Do check e-mail addresses carefully before sending an e-mail and do not just click through the external address pop-up screen checker.
- Do immediately bring to the attention of the Director of Finance and Corporate Services any subject access request which the organisation receives. A subject access request is a written request by or on behalf of any individual for a copy of any personal data which the organisation holds about that individual. There is no need for the person making the request to call it a "subject access request" or even to mention the Data Protection Act 1998.
- Do use common sense. The requirements of data protection legislation in many cases just reflect good data management practices and, as such, applying common sense is likely to be a good starting point in determining whether there will be an issue in a particular situation.

13.2 Don't

- Do not access personal data held by the organisation in any form, unless access is reasonably required for work purposes.
- Do not commit to writing (whether email, a Word document, a handwritten note or otherwise) or otherwise record any opinions about any individual(s) unless:
- it can be justified on reasonable grounds
- There would be no issue with the individual in question in each case viewing what has been written about them.
- Do not take laptops, memory sticks or other portable IT devices storing personal data out of CDN' offices unless they are encrypted.
- Do not dispose of hard copies of information containing personal data anywhere other than in CDN' offices, using the confidential waste bins provided.
- Do not disclose recipients' email addresses to all other recipients, when sending an email to more than one person, except if and to the extent that each recipient reasonably requires to have access to other recipients' email addresses, in light of the purpose and content of the email.

8 FAQs

8.1 *What happens if I do not adhere to this policy?*

Answer: By not adhering to the required timescales, for example, you may risk not getting your leave or pay paid/approved at a time that suits your needs and your family's needs. If in doubt about any stage of this Policy, please contact HR.