Information Security and Data Protection Policy

28 April 2017

The Data Protection Act 1998

Oxford HR processes personal data in relation to its own staff, candidates seeking a new appointment and individual client contacts - therefore it is a "*data controller*" for the purposes of the Data Protection Act 1998. Oxford HR has notified the Information Commissioner's Office – the Company's data protection registration number is Z1277648.

The Company holds personal data on individuals ("*data subjects*") for the following general purposes:

- Staff administration.
- Advertising, marketing and public relations.
- Accounts and records.
- Administration and processing of the personal data of candidates seeking new appointments and client contacts, for the purposes of leading the search and assessment process for the identification of new hires.

The eight principles of data protection

The Data Protection Act 1998 requires Oxford HR, as a data controller, to process data in accordance with the principles of data protection. These require that personal data shall be:

1. Fairly and lawfully processed.
2. Processed for limited purposes.
3. Adequate, relevant and not excessive.
4. Accurate.

5. Not kept longer than necessary.

6. Processed in accordance with the data subjects rights.

7. Kept securely.

8. Not transferred to countries outside the European Economic Area without adequate protection.

"*Personal data*" means data, which relates to a living individual who can be identified from the data or from the data together with other information, which is in the possession of, or is likely to come into possession of the Company.

"*Processing*" means obtaining, recording or holding the data or carrying out any operation or set of operations on the data. It includes organising, adapting and amending the data, retrieval, consultation and use of the data, disclosing and erasure or destruction of the data. It is difficult to envisage any activity involving data, which does not amount to processing. It applies to any processing that is carried out on computer including any type of computer however described, main frame, desktop, laptop, iPad, Blackberry ® or other mobile device.

Personal data should be reviewed on a regular basis to ensure that it is accurate, relevant and up to date and those people listed in the Appendix shall be responsible for doing this.

Personal data may only be processed with the consent of the person whose data is held. Therefore if they have not consented to their personal details being passed to a third party this may constitute a breach of the Data Protection Act 1998. By instructing Oxford HR to look for work and by providing us with personal data contained in a CV, work-seekers will be giving their consent to processing their details for work-finding purposes. When candidates apply for a job or register through our website they agree to the following: "Oxford HR will process and store all data in compliance with the UK Data Protection Act 1998 and Oxford HR's Data Protection Policy and Privacy Policy. Please tick the box below to give your consent that the information you have given on this form may be processed and stored in this way. If you intend to use their personal data for any other purpose you MUST obtain their specific consent in advance.

Caution should be exercised before forwarding the personal details of any individuals on whom personal data is held, to any third party such as past, current or prospective employers, suppliers, customers and clients, persons making an enquiry or complaint and any other third party.

Sensitive personal data

Personal data in respect of the following is "*sensitive personal data*" and any information held on any of these matters MUST NOT be passed on to any third party without the express written consent of the individual:

- Any offence committed or alleged to be committed by them.
- Proceedings in relation to any offence and any sentence passed.
- Physical or mental health or condition.
- Racial or ethnic origins.
- Sexual life.
- Political opinions.
- Religious beliefs or beliefs of a similar nature.
- Whether someone is a member of a trade union.

Information security

From a security point of view, only those staff listed in the Appendix are permitted to add, amend or delete personal data from the Company's database(s) ("database" includes paper records or records stored electronically). However all staff are responsible for notifying those listed where information is known to be old, inaccurate or out of date. In addition all employees should ensure that adequate security measures are in place. For example:

- Computer screens should not be left open by individuals who have access to personal data.
- Passwords should not be disclosed.
- Email should be used with care.
- Where a staff member uses their own computer or mobile device to access data when working remotely from the office, copies of data must not be saved to any such device.
- Personnel files and other personal data should be stored in a place in which any unauthorised attempts to access them will be noticed. They should not be removed from their usual place of storage without good reason.

- Personnel files should always be locked away when not in use and when in use should not be left unattended.
- Unintended or potential breaches of data security, such as loss of equipment where data is stored or from which data could be accessed, must be reported to Philip Nelson, Managing Director, immediately.
- Any breaches of security should be treated as a disciplinary issue.
- Care should be taken when sending personal data in internal or external mail.
- Destroying or disposing of personal data counts as processing. Therefore care should be taken in the disposal of any personal data to ensure that it is appropriate. Such material should be shredded or stored as confidential waste awaiting safe destruction.

It should be remembered that the incorrect processing of personal data e.g. sending an individual's details to the wrong person, allowing unauthorised persons access to personal data, or sending information out for purposes for which the individual did not give their consent, may give rise to a breach of contract and/or negligence leading to a claim against the Company for damages from an employee, work-seeker or client contact. **A failure to observe the contents of this policy will be treated as a disciplinary offence.**

Subject access requests

Data subjects are entitled to obtain access to their data on request and after payment of a fee. All requests to access personal data by data subjects should be referred to Zoe Millington, Business Manager, whose details are listed in the Appendix to this policy.

References

Any requests for access to a reference given by a third party must be referred to Philip Nelson, Managing Director, and should be treated with caution even if the reference was given in relation to the individual making the request. This is because the person writing the reference also has a right to have their personal details handled in accordance with the Data Protection Act 1998, and not disclosed without their consent. Therefore when taking up references an individual should always be asked to give their consent to the disclosure of the reference to a third party and/or the individual who is the subject of the reference if they make a subject access request. However if they do not consent then consideration should be given as to whether the details of the individual giving the reference can be deleted so that they cannot be identified from the content of the letter. If so the reference may be disclosed in an anonymised form.

The Human Rights Act 1998

Finally it should be remembered that all individuals have the following rights under the Human Rights Act 1998 and in dealing with personal data these should be respected at all times:

- Right to respect for private and family life (Article 8).
- Freedom of thought, conscience and religion (Article 9).
- Freedom of expression (Article 10).
- Freedom of assembly and association (Article 11).
- Freedom from discrimination (Article 14).

APPENDIX

Person responsible for responding to subject access requests:

Zoe Millington, Business Manager

Persons responsible for adding, amending or deleting data:

Philip Nelson, Managing Director

Thibaut Mills, Deputy Managing Director

Zoe Millington, Business Manager

Jamie Phillips, Associate Senior Researcher

Maria Grigore, Research and Business Development

Amel Alariqi, Researcher

Maria Laguna, Finance Manager

Catherine Whitmore, Associate Human Resources Consultant