OCRA (LONDON) LIMITED

Data Security Policy

OCRA (LONDON) LIMITED
3RD Floor
14 Hanover Street
London
W1S 1YH
United Kingdom
T : 0207 317 0600
F: 0207 317 0610
E privacy@ocra.co.uk
www.ocra.co.uk

Contents

1 Interpretation

1.1 The Definitions provided in the Company's Data Protection Policy apply equally to this Data Security Policy.

2 About this Policy

2.1 This Policy sets out the Company's approach to data security and should be read in conjunction with the Company's Data Protection Policy and other Privacy Policies.

2.2 This Data Protection Policy applies to all Company Personnel. All Company Personnel must read, understand and comply with this Data Protection Policy and the Company's Privacy Policies when Processing Personal Data on the Company's behalf and attend training provided on its requirements.

2.3 Any breach of this Data Protection Policy or other Privacy Policy may result in disciplinary action.

2.4 This Policy does not form part of any Contract between the Company and Company Personnel or the Company and any other third party (including clients, customers and agents).

2.5 This Data Protection Policy (together with Privacy Policies) should not be shared with third parties, clients or regulators without prior authorisation from the DPM.

3 Data Security

3.1 The Company will take appropriate security measures to protect against:

3.1.1 unlawful or unauthorised Processing of Personal Data; and

3.1.2 accidental loss of, damage to, or destruction of Personal Data

which apply from the point of collection to the point of destruction.

3.2 The Company maintains data security by protecting the confidentiality, integrity and availability of Personal Data by taking reasonable steps to ensure:

3.2.1 Personal Data is accurate and suitable for the purpose for which it is processed;

3.2.2 Personal Data is only stored on our central computer system instead of individual PCs;

3.2.3 all Company Personnel are bound by appropriate confidentiality obligations; and

3.2.4 all Company Personnel undertake regular training on secure information management and data protection.

4 Risk Assessment

4.1 The Company will regularly undertake risk assessments in relation to data security and in particular will undertake a risk assessment or Data Protection Impact Assessment in the event that it changes the basis of its current technology or introduces new technology which is likely to result in a high risk to the privacy of individuals.

5 Technical Security Measures

5.1 The Company will adopt such technical security measures as are proportionate to address identified risks to the security of Personal Data. These might include, for example:

5.1.1 secure configuration of new and existing hardware;

5.1.2 implementing firewalls and internet gateways;

5.1.3 implementing malware protection and patch management programmes;

5.1.4 backing up data;

5.1.5 restricting user access to systems and data to authorised Company Personnel.

5.2 All Company Personnel are required to co-operate with the Company and its IT Department in relation to the operation of such technical security measures. In particular, all Company Personnel must:

5.2.1 comply without delay with any requests or instructions in relation to the updating of IT systems;

5.2.2 not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties).

6 User Protocols

Equipment

6.1 Only Company equipment shall be used to access the Company's IT Systems (unless use of personal equipment is expressly authorised)

6.2 Personal use of the Company's IT Systems and equipment is not permitted unless expressly authorised by the Company's IT Department.

6.3 All Company Personnel shall be responsible for the security and safety of equipment (and information) belonging to the Company particularly when it is taken outside of the Company's premises.

6.4 All equipment damaged or lost must be reported to the Company's IT Department without delay.

6.5 Company equipment may only be disposed of by the IT Department, which will arrange for secure disposal.

6.6 On leaving the Company's employment all Company equipment (and passwords) must be delivered to the Company's IT Department.

Work Station Security

6.7 From time to time the Company will issue protocols in relation to work station security. All Company Personnel must comply with such protocols and, in particular, must:

6.7.1 Lock or log off work terminals on leaving the work station and log off and switch off all terminals at the end of the working day;

6.7.2 Not allow unauthorised persons to use work terminals or access the Company's IT Systems;

6.7.3 File away all papers and manual data in a designated secure place at the end of the working day;

Usernames and Passwords

6.8 From time to time the Company will issue protocols in relation to the setting of passwords for use of its IT systems. All Company Personnel must comply with password protocols and, in particular:

6.8.1 must keep confidential any username or password and not write down a password or share it; and

6.8.2 must not use any other person's username or password or allow any other person to use their username or password;

6.8.3 must not access or attempt to gain access to restricted areas of the network or to any password protected information (except in the proper performance of duties).

IT System Security

6.9 From time to time the Company will issue protocols in relation to system security. All Company Personnel must comply with such protocols and, in particular, must not:

6.9.1 open attachments to emails unless confident that the attachment is from a safe source. Such emails should not be opened and should be notified to the IT Department;

6.9.2 access internet pages unless satisfied that the website is safe;

6.9.3 download or install software from external sources without authorisation from [the IT Department]. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked by [the IT Department] before they are downloaded;

6.9.4 attach any device or equipment to the Company's systems without authorisation from the IT Department; this includes any USB flash drive, MP3 player, tablet, smartphone or other similar device, whether connected via the USB port, infra-red connection or in any other way;

6.9.5 connect to any wifi outside of the Company unless it is your own personal wifi which is password protected. If you require internet access whilst working off site, please speak to the IT Department.

6.10 You must notify the IT Department urgently if you suspect that any virus or other software has been downloaded to the Company's systems. If in doubt about whether any act or omission may affect the security of the Company's IT system, you should seek guidance and advice from the Company's IT Department without delay.

Relevant Policies

6.11 From time to time the Company will issue additional protocols and policies in relation to data security. All Company Personnel must comply with such protocols and, in particular, must comply with the following relevant policies:

6.11.1 The Company's Document Retention Policy (Schedule 1 to the Data Protection

Policy)

6.11.2 The Company's Data Breach Policy

6.11.3 The Company's Data Security Policy

7 Data Security Techniques

7.1 All Company Personnel are responsible for considering whether there are opportunities in the context of their own role to enhance data security by adopting and of the following techniques:

7.1.1 **Data Minimisation**: Personal Data collected and retained must be the minimum amount of data required for the particular purpose for which it is collected. Where Personal Data is inaccurate or no longer relevant or required, Company Personnel are required to take steps to correct, destroy, or delete such data in accordance with the Company's Data Retention Policy.

7.1.2 **Encryption:** Sensitive data or highly confidential should where possible be encrypted both in storage and particularly on transfer to third parties

7.1.3 **Anonymisation:** Data ceases to be Personal Data where the information identifying a particular Data Subject is irreversibly removed. Where the identity of a Data Subject is not relevant to the Company's purpose, anonymisation will improve data security.

7.1.4 **Pseudonymisation:** The security of Personal Data can be improved where the information that identifies an individual (e.g. name) is replaced by an artificial identifier or pseudonym (e.g. a number) so that the Data Subject to which the Personal Data relates can no longer be identified, without the use of additional information kept separately and securely.

8 Data Sharing

Confidentiality

8.1 All Company Personnel are obliged to keep certain types of Company information including Personal Data and Sensitive Personal Data confidential. Particular care should be taken when Company Information is taken or may be viewed outside of the Company's premises. You should avoid accessing Company information in places or at times where the public or other third parties may have unauthorised sight or access to Company information.

Third Parties

8.2 Data should not be disclosed or transferred to third parties unless such disclosure or transfer is made:

8.2.1 in accordance with the Company's Data Subject Request Policy;

8.2.2 in circumstances where there are appropriate terms and conditions in place; or

8.2.3 in circumstances where the third party has appropriate data security safeguards in place

8.3 Data Transfers Data must not be transferred to a country outside of the EEA without ensuring

that appropriate safeguards are in place to ensure an adequate level of data security. Any such cross border transfer shall be in accordance with the Company's Data Protection Policy and in accordance with guidance issued by the Company's DPM from time to time, which must be sought if in any doubt about what security measures are required.

9 Monitoring

9.1 The Company will monitor use of Company IT Systems by Company Personnel for the purpose of security and to ensure that systems are used in accordance with this Policy and the Company's other Privacy Policies.

10 Testing, Review and Audit

10.1 The Company will undertake testing of its systems, including penetration testing, to ensure the security of Personal Data.

10.2 The Company will review and audit its systems and protocols and compliance with them on a regular basis.

11 Changes to this Policy

11.1 The Company reserves the right to change this Data Security Policy at any time without notice. It is your responsibility to ensure that your knowledge of this Data Security Policy is up to date and that you comply with its terms.