



Ixion Group

**Data Protection:
Employee Record Policy**

INTRODUCTION

The Ixion Group of companies (Ixion) fully respects your right to privacy. However in order for us to carry out our business, we need to collect, use, and keep personal data on our employees (data subjects).

Ixion Holdings Ltd acquired Computer Gym (UK) Limited - now called Ixion CG Limited - in April 2010, and is actively working towards implementing this policy throughout this multi-site company.

The Data Protection Act 1998 (the 'Act') regulates the way in which certain information about data subjects is held and used. We at Ixion fully accept our responsibilities and adhere to all UK data protection and freedom of information legislation.

DEFINITION OF PERSONAL DATA

Personal data is defined by the Act as data which relates to a living individual who can be identified from that data, or from that data and other information which is held by the company.

The Act also defines "sensitive personal data" as personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; trade union membership; their physical or mental health condition; their sexual life; the commission or alleged commission by them of any offence; or any proceedings for any offence committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

RIGHTS OF DATA SUBJECTS

Under the Act, data subjects have the following rights:

- To be informed that their personal data is being processed;
- To access any of their personal data held by the Company within 40 days of making a request;
- To prevent the processing of their personal data in limited circumstances; and
- To rectify, block, erase or destroy incorrect personal data.

PRINCIPLES OF DATA PROTECTION

Any personal data which Ixion collects, records or uses in any way – whether it is held on paper, on computer or other media – will have appropriate safeguards in place to ensure that Ixion complies with the Act. Ixion fully endorses and adheres to the eight principles of the Act, which state that personal data:

1. Must be processed fairly and lawfully (and shall not be processed unless certain conditions are met);
2. Must be obtained only for specified and lawful purposes;
3. Must be adequate, relevant and not excessive with respect to the purposes for which it is processed;
4. Must be accurate and, where appropriate, kept up to date;
5. Must be kept for no longer than is necessary in light of the purpose(s) for which it is processed;
6. Must be processed in line with your rights;
7. Must be secure so that it is protected against unauthorised or unlawful processing, accidental loss, destruction or damage; and
8. Must not be transferred to a country or territory outside of the European Economic Area without adequate protection.

PURPOSES FOR WHICH INFORMATION IS HELD

Throughout your employment, and for as long a period as is necessary following termination of your employment, the Company will need to keep information about you for purposes connected with your employment, including your recruitment and the termination of your employment. The information we hold will be for our management and administrative use. Only employees specifically required and entitled to access confidential information, as a result of their job function, may do so. All other employees are prohibited from accessing, reading, copying or in any other way dealing with such information. We believe these uses are consistent with our employment relationship and with the principles of the Data Protection Act 1998.

TYPE OF INFORMATION HELD

The records may include: information gathered from you and any confidential references obtained during your recruitment; details of your terms of employment; payroll, tax and national insurance information; performance appraisals; details of your job duties and job/salary band; health records; absence records including self certification forms; details of any disciplinary records; training records; contact names and addresses; correspondence with the Company and other information that you may have given to the Company.

HEALTH RECORDS

The Company may hold information about your health for the purposes of compliance with our health and safety and occupational health obligations; for the purposes of personnel management and administration, for example, to consider how your health affects your ability to do your job and, if you have a disability, whether you require any reasonable adjustments to be made to assist you at work; and the administration of insurance, pension, sick pay and any other related benefits.

Data under this heading may be revealed to relevant senior managers and Human Resources only; and will not be revealed to fellow employees and peers (unless those employees are responsible for health records in the normal course of their duties).

Employees have the right to request that the Company does not keep health records on them. All such requests must be made in writing and addressed to the HR Co-ordinator at Ixion Holdings, or the Corporate Services Director at Ixion CG.

DISCLOSURE OF INFORMATION HELD TO A THIRD PARTY

From time to time, we may need to disclose some information we hold about you to relevant third parties (e.g. where requested to do so by you for the purpose of giving a reference).

Prior to disclosure – unless it is a legal obligation (e.g. data required by HM Revenue & Customs) – employees will be fully informed of the personal data that is being disclosed, the reasons for the disclosure, and the way(s) in which it will be processed.

MONITORING

The Company may from time to time monitor the activities of employees. Such monitoring may include, but will not necessarily be limited to, internet and email monitoring. Any employee to be monitored will be informed in advance.

Under no circumstances will monitoring interfere with an employee's normal duties.

The Company shall use its best and reasonable endeavours to ensure that there is no intrusion upon employees' personal communications or activities and under no circumstances will monitoring take place outside of the employee's normal place of work or work hours.

DATA PROTECTION PROCEDURES

The Company will ensure that all of its employees working on behalf of the Company comply with the following when processing and/or transmitting personal data:

- All emails containing personal data must be encrypted;
- Personal data must be transmitted over secure networks only – transmission over unsecure networks is not permitted in any circumstances;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated with the email should also be deleted;
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient. Using an intermediary is not permitted;
- All hard copies of personal data should be stored securely in a locked box, drawer, cabinet or similar;
- All electronic copies of personal data should be stored securely using passwords and suitable data encryption, where possible on a drive or server which cannot be accessed via the internet; and
- All passwords used to protect personal data should be changed regularly and should not use words or phrases which can be easily guessed or otherwise compromised.

EMPLOYEE ACCESS TO INFORMATION

Subject to certain conditions, the Act provides that an individual has the right, **on written request**:

- to be informed whether personal data about him/her is being processed, whether by the employer or someone else on its behalf;
- to be given a description of the purposes for which personal data is being processed; and details of all recipients/classes of recipients to whom it is or may be disclosed;
- to have communicated, in an intelligible form, any information held about him/her by the employer, as well as any information available to the employer as to the source of this information;
- to be informed of the logic involved in computer-assisted decision making, for instance psychometric testing.

EMPLOYEE PROCEDURE FOR MAKING A SUBJECT ACCESS REQUEST

The Act provides that an employer does not have to supply an employee with copies of the personal data held unless:

- a written subject access request is received (the request should be addressed to the HR Co-ordinator at Ixion Holdings, or the Corporate Services Director at Ixion CG);
- the employer is supplied with any information reasonably required to confirm the identity of the person making the request;
- an identical or similar request by the same individual has been made without a reasonable time interval lapsing.

WHAT INFORMATION WILL BE DISCLOSED TO THE EMPLOYEE IN RESPONSE TO A SUBJECT ACCESS REQUEST?

In response to a proper request, employees are entitled to be given access (in the presence of the HR Co-ordinator at Ixion Holdings, or the Corporate Services Director at Ixion CG) to all the personal data held (excepting exempt data items) relating to them that is available at the time the request is received.

Employees can request, at the time of viewing the personal data held, to be given copies of the data in a permanent form.

EXEMPT DATA ITEMS

There is no requirement for data items that are exempt from the subject access provisions to be disclosed. They will therefore be removed from the employee's file on receipt of a written subject access request. Such items will include:

- Confidential employment references given or to be given by the employer;
- Management forecasts/planning e.g. succession planning or proposed redundancies;
- Negotiations with the employee e.g. pay increases, promotion or severance packages;
- Information provided in confidence by a third party e.g. information provided to assist a disciplinary investigation;
- Legal advice i.e. a confidential communication between the employer and its legal adviser;
- National security, crime and taxation data;
- Disclosures required by law.

DO EMPLOYERS HAVE TO RESPOND TO SUBJECT ACCESS REQUEST IMMEDIATELY?

Employers have 40 days in which to respond to a subject access request, beginning with the day on which a proper request was received. However it is our policy, as far as is reasonably practicable, to provide employees with access to personal data within 5 working days.

SUBJECT ACCESS REQUEST

If you have any queries about the procedure for making a subject access request, please speak to the HR Co-ordinator at Ixion Holdings, or the Corporate Services Director at Ixion CG.

RESPONSIBILITY FOR IMPLEMENTATION OF THIS POLICY

The people responsible for data protection in the Ixion Group are the Data Controllers Chris Adams who is based at Ixion Holdings in Chelmsford, and Pat Phillips, who is based at Ixion CG in Epsom.

If you have any queries or concerns, please contact Chris Adams at Chelmsford on 01245 241442 or Pat Phillips at Epsom on 0844 8008885.

RESPONSIBILITY FOR MONITORING THIS POLICY

This policy will be reviewed annually (or more frequently, if legislation and/or best practice make it necessary) by the Data Controllers in order to ensure its continuing relevance.

The Group CEO is responsible to the Ixion Holdings Board for the policy

Any changes to the policy will be communicated to all employees.

DATA PROTECTION REGISTER

As we are a Company that processes personal data, we are required to be registered with the Information Commissioner's Office, which is an independent authority that regulates and enforces the Act.

All companies must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence.

It is our Data Controller's responsibility for the annual renewal. Our Data Protection Register numbers are as follows:

Ixion Holdings:	Z9405579
Ixion CG:	Z7705560