# ENFIELD INNOVATIONS LTD

# DATA PROTECTION POLICY

Adopted August 2015

# CONTENTS

# 1. INTRODUCTION

1.1 Enfield Innovations Ltd (EIL) is required, as part of its overall information governance structure, to ensure that appropriate controls are implemented and maintained in relation to the collection, use and retention of personal information pertaining to its customers, clients and staff and that these are in accordance with the requirements of the Data Protection Act 1998 (DPA).

1.2 This document provides a framework for EIL to meet legal requirements in relation to information requests that fall within the scope of the DPA legislation.

1.3 The Policy applies to all personal information created, received, stored, used and disposed of by EIL irrespective of where or how it is held.

1.4 It must be noted that the DPA is a 'legal' requirement and that individuals can face prosecution for breaches of its Principles and can be fined as individuals.

# 2. AIM OF POLICY

2.1 The aim of this document is to clarify EIL's legal obligations and requirements for the processing of personal data and to ensure that all such data is:

- collected, stored and processed for justifiable business reasons
- used only by those persons with a legitimate reason
- stored safely
- retained only for the defined time period
- not disclosed to unauthorised persons.

2.2 EIL will actively seek to meet its obligations and duties in accordance with the DPA and in so doing will not infringe the rights of its employees, customers, third parties or others.

## 3. SCOPE

3.1 The scope of this policy requires compliance with the Data Protection Principles which are defined in the DPA.

**Personal Data** is defined as: personal data relating to an identifiable living individual and includes the expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

**Sensitive personal data** is defined as personal data consisting of information as to:

- racial or ethnic origin
- political opinions
- religious or other beliefs
- trade union membership
- physical or mental health or condition
- sexual life
- commission of criminal offences or alleged offences.

3.2 Extra protection needs to be given to sensitive personal information and it may require additional security measures to ensure both its integrity and security.

## 4. DATA PROTECTION PRINCIPLES

4.1 The DPA is underpinned by a set of eight common-sense principles, which must be adhered to whenever personal data is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal data.

4.2 All personnel processing personal information in the course of their business functionality must ensure they adhere to the eight Data Protection Act principles which requires that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- Be adequate, relevant and not excessive for those purposes
- Be accurate and kept up-to-date
- Not be kept longer than is necessary for that purpose
- Be processed in accordance with the data subjects' rights

- Be kept safe from unauthorised access, accidental loss or destruction

- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

4.3 Further information on the data protection principles can be found on the Information Commissioner's Office website.

## 5 THE INFORMATION COMMISSIONER'S OFFICE

5.1 The Information Commissioner administers the Data Protection Act. The role and duties of the Commissioner include:

- ensuring compliance with the Act

- ensuring that individuals rights to privacy are respected

- ensuring that individuals have access to data held about themselves

- establishing and maintaining a Register of data users and making it publicly available

- investigating complaints, serving notices on registered data users who are contravening the principles of the Act, and where appropriate prosecute offenders.

5.2 The Act gives the Information Commissioner wide powers to ensure compliance with the Act, including warrants to search and seize documents and equipment.

## 6 ACCESS AND USE OF PERSONAL DATA

6.1 This policy applies to everyone that has access to personal data, and includes any third party or individual who conducts work on behalf of EIL or who has access to personal data for which EIL is responsible and who will be required contractually or otherwise to comply with this policy.

6.2 Deliberate unauthorised access to, copying, disclosure, destruction or alteration of or interference with any computer equipment or data is strictly forbidden and may constitute a criminal and/or a disciplinary offence.

6.3 It is an offence under Section 55(1) of the Data Protection Act, for any person to knowingly or recklessly obtain, procure or disclose personal data, without the permission of the data controller (EIL) subject to certain exceptions.

6.4 It is also an offence for someone to sell or offer to sell personal data which has been obtained in contravention of Section 55(1). Full details of this offence can be found under Section 55 of the Data Protection Act 1998.

6.5 All personnel (staff or customers) are entitled to:

- Know what information EIL holds and processes about them and why it is held
- Know who can gain access to it
- How to keep this data up-to-date
- Know what action EIL takes to comply with its obligations under the DPA.

6.6 EIL will ensure that compliance with this Policy is monitored and is able to evidence that it is complying with its legal responsibilities with respect to its staff and customers.

# 7 ENFIELD INNOVATION'S COMMITMENT

7.1 To achieve the overall aim of the Data Protection Policy, EIL will:

- Provide adequate resources to support an effective corporate approach to Data Protection
- Respect the confidentiality of all personal information irrespective of source
- Publicise EIL's commitment to Data Protection on the company website once created
- Compile and maintain appropriate procedures and codes of practice
- Promote general awareness and provide specific training, advice and guidance to its staff at all levels and to its Members to ensure standards are met
- Monitor and review compliance with legislation and introduce changes to policies and procedures where necessary.

# 8 ROLES AND RESPONSIBILITIES

8.1 Ultimate accountability for all decisions made relating to the Data Protection Act 1998 and associated legislation lies with the **Board of Directors**.

8.2 The **Board of Directors** is responsible for ensuring that sufficient resources are provided to support the requirements of this policy as well as making strategic level decisions which impact on how EIL carries out its obligations under the legislation. Each Director is responsible for monitoring compliance and taking any necessary corrective action.

8.3 **Information/System Owners** have a responsibility to ensure that data stored on systems is captured, stored, processed, accessed and deleted in line with the Data Protection Act.

8.4 **All EIL employees** and personnel working with personal data have a responsibility to ensure that they have sufficient awareness of the DPA so that they are able to comply with the requirements of the DPA.

# 9 RESPONSIBILITIES OF STAFF, DIRECTORS & THIRD PARTY CONTRACTORS

9.1 The processing of personal data is to be compliant with legal, industry, regulatory and business requirements; it is the responsibility of staff, Directors and third party organisations providing services on behalf of EIL to be aware of and conversant with these requirements for the processing and management of personal data in an appropriate manner.

9.2 Staff, Directors and third party organisations providing services on behalf of EIL will need to be aware of how staff, Directors and third party organisations providing services on behalf of EIL safeguards its data and ensure that the appropriate protective marking is applied to all information. In most cases personal information about any living individual will attract the classification of PROTECT**,** but in some cases it will be RESTRICTED, for example when large quantities of sensitive information are grouped together, or where the information could put someone at risk.

9.3 The following minimum requirements are applied to everyone who comes into contact with personal data:

- Ensure that personal data is to be processed accurately and only for a specific purpose. If data needs to be used for a different purpose then the consent process will need to be repeated

- When not required for immediate use personal data is to be secured from unauthorised viewing and access

- Personal, sensitive and restricted data must not be sent to/from personal/staff/member home email accounts

- Personal information can only be distributed externally through email if it is:
  - password protected and encrypted or
  - via the GCSX email within the GCSX network of users or
  - via a Secure Enhanced File Transfer facility.

- Computer systems that process, access or store such data are to have password protected screen savers activated when left unattended.

- The carrying of personal, sensitive or confidential information outside secure office environments should be avoided wherever possible. If this is unavoidable, then staff, Directors and third party organisations providing services on behalf of EIL should use encrypted laptops where possible. Documents holding personal or sensitive information should be carried separately to the laptop case.

- When no longer required to be retained all personal data is to be disposed of securely, i.e. by shredding or via secure waste disposal.

- Personal data may not be stored on removable media devices without explicit management approval and appropriate encryption controls. Such data is to be removed from the removable media as soon as practically possible.

- The discussion of personal data with unauthorised persons either inside or outside EIL is expressly prohibited. This also includes, but is not limited to, email, social networking sites, blogs, forums, instant messaging services, chat rooms etc.

- Any staff directly employed by EIL will be required to undertake Data Privacy and Information Security training on joining the organisation and as required thereafter. Any staff employed by Enfield Council providing services to EIL via Service Level Agreements will need to have completed Data Protection and Information Security training at the Council.

## 10 DATA CONTROLLER

10.1 In accordance with the DPA, EIL as a corporate body is the Data Controller and is therefore ultimately responsible for the implementation of this policy.

10.2 EIL staff responsible for the day-to-day management of the data within their business areas of responsibility are required to ensure that:

- all data is processed fairly

- the data is accurate, and that processes exist to check and amend data as necessary

- consent is obtained either generally or expressly and that a data subject is not misled/deceived as to why their data has been collected

- policies and procedures are in place to enable access by those who the data concerns and data subjects should be advised who is holding and using their data

- data is held securely
- data is disposed of properly
- notification requirements are satisfied
- determination regarding processing of data without consent are made, especially in cases of public interest.

## 11 DATA PROTECTION OFFICER (DPO)

11.1 The DPO is responsible for EIL's registration with the Information Commissioners' Office (ICO), and for ensuring EIL complies with current legislation. The DPO is the Company Secretary.

11.2 The DPO will monitor that appropriate 'fair processing' statements are made when EIL, its agents, contractors or service providers collect or process personal information for which EIL is the Data Controller, reflecting the purposes for which the information may be used and any other parties to whom the information may be revealed (Principle 1).

11.3 The DPO will monitor periodic reviews of computer and hard copy records to verify that the personal information held is:

- adequate, relevant, and not excessive for its purpose (Principle 3);
- accurate and up to date (principle 4); and
- not kept for longer than is necessary (principle 5).

11.4 The DPO will respond to complaints about how we have processed personal information relating to individuals; this must be within 21 days of receipt. The response must explain the actions (if any) LBE will take.

11.5 The DPO will keep Directors and any directly employed staff informed of data protection issues pertaining to EIL, including any changes in legislation that might impact business processes.

11.6 The DPO will ensure that Data Privacy and Information Security training is available to staff and that a record of completion is maintained.

11.7 The DPO must be made aware of any proposed new or changed uses of personal information before any change in process or additional information collection is authorised.

11.8 If a member of staff or customer (or an authorised person acting on their behalf) submits a Subject Access Request (SAR) regarding the personal information held about them the DPO must ensure that relevant staff are aware of the separate guidance note on responding to a SAR the key points of which are highlighted below:

- the request is made in writing;
- the claimants identity has been verified (or approval for a 3rd party to act on their behalf);
- whether or not the request is restricted to information held for specific purposes;
- that the appropriate fee has been paid
- the request is logged and then closed with timescales monitored.

11.9 The DPO is responsible to ensure that SAR's are processed within 40 days of receipt, collating relevant information and for clarifying what information, if any, is to be provided (Principle 6).

## 12. TRAINING AND AWARENESS

12.1 All direct EIL employees have a responsibility to ensure that they and the staff they manage have undertaken Data Privacy and Information Security training and have sufficient awareness of the DPA so that they are able to comply with the requirements.

12.2 It is mandatory that all EIL staff (including temporary or casual workers) that have access to personal data or to the corporate network to undertake the Data Privacy and Information Security training. New entrants will be expected to undertake and successfully complete the module as part of the corporate induction process. Established staff will be expected to undertake and complete refresher training as directed.

12.3 Managers should encourage and make time for their staff to attend any further Data Privacy and Information Security training or awareness opportunities that may arise.

12.4 Failure to complete the courses within the prescribed period could result in disciplinary action proceedings.

## 13. COLLECTION OF DATA

13.1 EIL collects and records personal data from various sources, including that obtained or provided by the data subjects themselves.

13.2 In some instances data may be collected indirectly through monitoring devices, including but not limited to: door access control systems, CCTV and physical security logs, electronic monitoring systems.

## 14. ACCURACY AND RELEVANCE

14.1 It is the responsibility of those who receive personal information to ensure so far as possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to ensure that it is still accurate.

14.2 If the information is found to be inaccurate, steps must be taken to rectify it. Individuals who input or update information must also ensure that it is adequate, relevant, unambiguous and professionally worded. Data subjects have a right to access personal data held about them and have inaccuracies corrected.

## 15. RIGHTS TO ACCESS INFORMATION

15.1 Employees and customers have the right to access any personal information (data) about them that is held or processed on computer or in certain hard copy files. Before access to this data is authorised a Subject Access Request form is to be completed and handed to an approved officer for processing.

15.2 EIL reserves the right to make an administration charge of £10 (ten pounds) on each occasion that access is requested; this is in addition to the direct costs of providing any copies of data.

15.3 EIL aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 40 days unless there is a good reason for any delay. In such cases the reason for a delay will be explained in writing to the person making the request.

## 16. FAIR AND LAWFUL PROCESSING

16.1 When EIL processes personal data, it must have a lawful basis for doing so. The DPA provides a list of conditions to ensure that personal information is processed fairly and lawfully:

- Personal information is only processed where it is justified, in accordance with Schedule 2 of the DPA

- That sensitive personal information is processed only where necessary and justified, that such processing is undertaken only by the appropriate persons in accordance with Schedules 2 and 3 of the DPA.

16.2 Individuals that supply EIL with personal information are provided with a ‘Privacy Notice’ (or online privacy statement) which communicates the following:

- The identity of the organisation

- The purpose(s) for which personal information will be processed
- Information regarding the disclosure of personal information to third parties
- Information regarding the individuals right of access to personal information
- Whether personal information is transferred outside the EEA
- Details of how to contact EIL with specific questions or queries regarding the processing of personal information
- Details of any specific technologies or electronic measure to collect information about individuals, i.e. website cookies.

## 17. DATA SHARING

17.1 Where EIL shares personal information with any third party a 'Data Sharing Agreement' is to exist as part of a formally documented written agreement or contract.

17.2 Where the other party uses the personal information for its own purposes:

- The agreement or contract will clearly describe the purposes for which the information may be used and any limitations or restrictions on the use of that information
- The other party is to provide an undertaking or provide other evidence of its commitment to process the information in a manner that will not contravene the DPA.

17.3 Where the processing of personal information with a third party is required by law, procedures are to ensure that the protocols and controls for the sharing of the data are documented, regularly reviewed and verified.

17.4 Requests for personal information from the Police or other enforcement agencies can be considered where the purpose is for the prevention or detection of a crime and or the collection of taxes (Section 29 DPA 1998). It should be noted however that EIL is under no obligation to do so. Before providing the information, the requesting agency must provide a sufficient explanation of why the information is necessary to the extent that not providing it may prejudice an investigation. This is to satisfy the relevant information holder that the disclosure is necessary. The request must be on letter headed paper and authorised by a senior officer from the requesting agency (Police Inspector or equivalent). If the information is to be disclosed, the disclosure must be authorised by the relevant Head of service (or above) and a note for the record should be made of the details about the disclosure with an explanation of why the disclosure is appropriate.

## 18. DATA RETENTION AND DISPOSAL

18.1 EIL is to ensure that personal information is not kept for any longer than is necessary; this is to adhere to any legal, regulatory or specific business justification.

18.2 EIL will retain some forms of information longer than others, but all decisions are to be based upon business requirements.

18.3 Data relating to clients is only to be retained for as long as a business justification remains.

18.4 When disposing of information, equipment or media, this should be done confidentially.

## 19. TRANSFER OUTSIDE OF THE EEA

19.1 To ensure an adequate level of protection is applied to personal information transferred or processed outside the European Economic Area (EEA) contracts are to include conditions relating to the specific requirements for the protection of the information.

19.2 EIL is responsible for ensuring that ‘due diligence’ is conducted on the other party, and that adequate and appropriate controls and safeguards are applied for the transfer of the personal information.

19.3 Companies outside the EEA are to be required to apply the same controls and requirements as applied within the EEA unless they can demonstrate other adequate procedures are implemented to protect the personal information as part of the ‘due diligence’ process. Periodic reviews of the same are to be conducted to ensure adherence is maintained.

## 20. VIOLATIONS

20.1 Unauthorised disclosure of personal data is a disciplinary matter that may be considered a gross misconduct and could lead to termination of employment.

20.2 In the case of third parties unauthorised disclosure could lead to termination of the contractual relationship and in certain circumstances this could give rise to legal proceedings.