Data Protection Policy

Document Control for Policy	
Supersedes	Supersedes: Version 4.0 Significant changes: New Document
Created / Updated by	Name: Siobhan Breslin Designation: Business Manager
Application	All paid staff and volunteers
Issue date	Date: May 2018 Circulated By: BreatheHR / Shared Drive
Footer updated	√

CONTENTS

1 Introduction

- First Light holds personal data about candidates, employees, clients, contacts, suppliers and other individuals for a variety of business purposes.
- This policy sets out how First Light seeks to protect personal data and ensure staff understand the rules governing their use of personal data to which they have access in the course of their work.
- In particular, this policy requires staff to ensure that the DPO should be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.
- The DPO is responsible for the monitoring and implementation of this policy. If you have any questions about the content of this policy or other comments you should contact the DPO.

2 Scope

- This policy applies to all staff, which for these purposes includes employ-ees, trainees, contractors and all others.
- All staff must be familiar with this policy and comply with its terms.
- This policy supplements First Light's other policies relating to data protection.
- First Light may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

3 Definitions

In this policy:

business purposes

- means the purposes for which personal data may be used by First Light, e.g. client services, personnel, administrative, financial, regulatory, payroll and business development

personal data

- means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location da-ta, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

special categories of personal data

- means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Any use of special categories of personal data must be strictly controlled in accordance with this policy

processing

- means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by auto-mated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4 General principles

First Light's policy is to process personal data in accordance with the applicable data protection laws and rights of individuals as set out below. All employees have personal responsibility for the practical application of First Light's data protection policy.

5 Lawfulness, fairness and transparency principle

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
- This principle is reflected in First Light's Fair Processing Notices.

6 Purpose limitation principle

- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes ('purpose limitation').

- Staff should make sure data processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one

purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

7 Data minimisation principle

- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
- Staff will ensure that they only process what personal data is required for their purpose and no more.

8. Accuracy

- Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').
- Individuals may ask First Light to correct personal data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the DPO who will investigate the situation accordance with this policy.

9. Storage limitation principle

- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the ap-propriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').
- Personal data should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances including the reasons why the personal data were obtained. Staff should follow First Light's data retention policy.

10 Integrity and confidentiality principle

- Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
- Staff must keep personal data secure against unauthorised or unlawful processing and against accidental loss, destruction or damage in accordance with First Light's information security policies.
- Where First Light uses external organisations to process personal data on its behalf additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. Staff should consult the DPO to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement.

11 Rights of access

- All persons, including staff, shall have the right to obtain from First Light confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and information regarding it.
- All Subject Access Requests should follow First Light's Subject Access Request policy and procedure.

12 Right of rectification

- All persons, including staff, shall have the right to obtain from First Light without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- All requests for rectification should follow First Light's rectification policy and procedure.

13 Right of erasure ('right to be forgotten')

- All persons, including staff, shall have the right to obtain from First Light the erasure of personal data concerning him or her without undue delay and First Light shall have the obligation to erase personal data without undue delay in certain circumstances.
- All requests for erasure should follow First Light's erasure policy and procedure.

14 Right to restriction of processing

- All persons, including staff, shall have the right to obtain from First Light restriction of processing in certain circumstances.
- All requests for restriction of processing should follow First Light's restriction of pro-cessing policy and procedure.

15 Notification obligation regarding rectification or erasure of personal data or restriction of processing

- First Light shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

16 Right to data portability

- All persons shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, if the data is processed based on consent or contract and where the processing is carried out by auto-mated means.
- First Light does not process any personal data by automated means and, therefore, cannot satisfy the right to data portability.

17 Right to object

- All persons, including staff, shall have the right to object to First Light processing his or her personal data if the processing is based on legitimate interest. In this case, First Light shall no stop processing the personal data unless First Light demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the person or for the establishment, exercise or defence of legal claims.
- Persons have the right to object to First Light processing their personal data for direct marketing purposes. Where a person does object, staff should notify the DPO. The per-son's email address will be moved to a suppression list so that they will not receive any further marketing material.

- Staff should not send direct marketing material to someone electronically (e.g. by email) unless there is an existing business relationship with them in relation to the services being marketed.
- Staff should contact the DPO for advice on direct marketing before starting any new direct marketing activity.

18 Automated decision making, including profiling

- All persons, including staff, shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
- First Light does not use any automated decision making.

19 Processing of special categories of data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited unless:

a) the person has given explicit consent to the processing of those personal data for one or more specified purposes;
b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
c) processing is necessary to protect the vital interests of the data subject or of an-other natural person where the data subject is physically or legally incapable of giving consent;
d) processing relates to personal data which are manifestly made public by the data subject;
e) processing is necessary for the establishment, exercise or defence of legal claims;
f) processing is necessary for the purposes of preventive or occupational medicine, for the
assessment of the working capacity of the employee.

Staff should not process any special categories of data without consulting the DPO.

20 Processing of personal data relating to criminal convictions and offences

First Light does not process personal data relating to criminal convictions.

21 Legal basis for processing

First Light uses the following legal basis for the processing of personal data:

a) consent – the person has consented to the processing of his or her personal data for one or more specific purposes;

b) contract – the processing is necessary for the performance of a contract to which the person is party or in order to take steps at the request of the person prior to entering into a contract;

c) legal obligation – the processing is necessary in order for First Light to comply with a legal obligation;

d) vital interests – the processing is necessary in order to protect the vital interests of the person;

e) legitimate interests – the processing is necessary for the purposes of the legitimate interests pursued by First Light or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of a person.

First Light explains the use of these legal basis in its Fair Processing Notices.

22 Consent

- Where First Light bases its processing on consent, First Light shall be able to demonstrate that the person has consented to processing of his or her personal data.
- Consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language
- A person, including staff, shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. It shall be as easy to withdraw as to give consent.
- Consent is not freely given if it is requested for a contract, but the processing of the personal data is not necessary for the performance of that contract.

23 Data protection impact assessment

- Where a type of processing, in particular using new technologies, and taking into ac-count the nature, scope, context and purposes of the processing, is likely to result in a high risk

to the rights and freedoms of natural persons, First Light shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

- The DPIA will be overseen by the DPO.

24 International transfer

- Personal data shall not be transferred outside the EEA (which includes the EU countries, Norway, Iceland and Liechtenstein) without appropriate safeguards.
- Staff should not transfer personal data outside of the EU or the EEA without first consulting the DPO.

25 Reporting breaches

Staff have an obligation to report actual or potential data protection compliance failures to the DPO. This allows First Light to investigate the breach and take appropriate steps, following the breach notification policy.

26 Training

- First Light Ltd takes the protection of personal data very seriously and therefore, all staff that process personal data will be trained according to their role requirements.
- Staff with any questions about data protection training should contact the DPO.

27 Consequences of failing to comply

- First Light takes compliance with this policy very seriously. Failure to comply puts both staff and First Light at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.
- Staff with any questions or concerns about anything in this policy should not hesitate to discuss these with [insert relevant department].

I have read and understood this policy and agree to abide by its terms.

Signed.....

Date ……..