FIRST LIGHT GENERAL DATA PROTECTION POLICY

INTRODUCTION

The General Data Protection Regulation 2018 ("The Regulation") provides rules which apply to the collection, use, disclosure and transfer abroad of information about individuals which includes employee and client personal data. The Regulation set out the principles that First Light must follow when processing personal data about individuals and also gives individuals certain rights in relation to personal data that is held about them.

The aims of this policy are:

- To assist First Light in meeting its obligations under The Regulation
- To regulate First Light's use of information relating to employees and others who work for First Light, and
- To ensure that employees and others working for First Light are aware of both their rights in relation to the personal data that First Light holds about them, and their responsibilities with regards to personal data they may process about clients and other individuals as part of their job

For ease of reference, this policy refers to "employees", but it applies equally to others working for First Light.

DEFINITIONS

Below are definitions under The Regulation:

DATA CONTROLLER: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to First Light Personnel and Personal Data used in our business for our own organisational purposes.

DATA PROCESSOR: 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

PERSONAL DATA: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

DATA SUBJECT: a natural person whose personal data is processed by a controller or processor

GENERAL DATA PROTECTION PRINCIPLES

The Regulation places an obligation on data controllers, such as First Light, to observe the data protection principles. In summary these include that personal data must:

- Be obtained and processed lawfully and fairly in order to serve a lawful purpose
- Be used and disclosed for specified, explicit and legitimate purposes and not in any manner incompatible with those purposes
- Be adequate, relevant and not excessive in relation the purposes for which they are processed
- Be accurate, complete and up-to-date, any information that is inaccurate in relation to purpose for which it is kept and processed, will be rectified or deleted without delay
- Not be kept for longer than is necessary for the purpose(s) for which it was obtained
- Be processed in line with the rights given to individuals under The Regulation
- Be kept safe and secure in line with The Regulation using the appropriate technical and organisational measures that will ensure appropriate security against unlawful processing and accidental loss, destruction or damage and
- Not be transferred to countries without adequate levels of data protection

All employees have an obligation to comply with these principles where appropriate and must ensure that all data stored by First Light is accurate.

WHAT IS PERSONAL DATA?

Personal data is data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. The data protection principles apply to any sort of personal data, which is either electronically processed (e.g. on a database) or which is held or intended to be in a structured filing system (e.g. a set of personnel files).

Certain personal data is classified as "sensitive personal data". This is personal data relating to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, physical or mental health, sexual life or any criminal offence or related proceedings. For example, First Light may, where necessary in connection with employment, collect and process sensitive personal data in respect of your health.

Any Personal Data processed by First Light will be kept secure in line with The Regulation and will only be kept for as long as it meets its required purpose.

FIRST LIGHT'S OBLIGATIONS

"Processing" includes the obtaining, recording, keeping and disclosing of data. Generally, processing of employee personal data may only be done with the employee's consent. However, such consent is not required in certain circumstances, for example where the processing is necessary for compliance with a legal obligation or where the processing is necessary for the performance of a contract to which the employee is a party e.g. an employment contract.

NATURE OF EMPLOYEE INFORMATION

First Light holds and processes certain personal information about you as part of its general employee records. The records may include your address, contact details, payroll details, educational history, position, etc. This sort of information is known as "personal data" under The Regulation. Employee information is also held on HR and operational databases. In some cases, the CEO / Manager might also hold employee information in their own files.

Sensitive personal data may include but is not limited to records of sickness absence, medical certificates and medical reports. The purpose of processing this type of information is generally to manage the application process, to administer benefit plans, to monitor and manage sickness absence and to comply with health and safety legislation. If sensitive personal data relating to you is being processed for reasons otherwise than those set out above or otherwise permitted by law, your explicit consent will be sought.

PURPOSE OF PROCESSING GENERAL EMPLOYEE INFORMATION

First Light needs to collect and use personal data about employees for a variety of personnel, administration, work and general business management purposes. These include administration of the payroll system, the administration of employee benefits (such as leave entitlements), facilitating the management of work and employees, carrying out appraisals, performance and salary reviews, operating and checking compliance with First Light's employment rules and policies, operating First Light's IT and communications systems, checking for unauthorised use of those systems and to comply with record keeping and other legal obligations.

KEEPING EMPLOYEE INFORMATION

First Light will take steps to ensure that the employee information it holds is accurate and up-to-date. For example, you will be asked to inform First Light of any changes which we need to make to update your employee information (such as a change of address). From time to time you will be asked to supply updated personal information as part of our annual review of personal data held to ensure that First Light meets its data protection obligations. First Light will also take steps to ensure that it does not keep any information about employees for longer than is necessary under the Regulation and other relevant legislation. First Light will put in place a policy for the archiving and/or removal of any personal data that is no longer required as per the relevant legislation and regulation in order to ensure data minimisation.

TRANSFER OF EMPLOYEE INFORMATION

First Light may make some information about you available to First Light's advisers and/or data processors such as lawyers, accountants, payroll administrators, benefits providers (for example, pension scheme providers), to those providing products or services to First Light (such as IT and other outsourcing providers) and to government and/or regulatory authorities. Personal data will only

be shared with such parties if they have a need to know the information for the purposes of providing the contracted services. These recipients may be located outside the European Economic Area. In this case, First Light will agree that the recipients of the information, both within and outside First Light, comply with the contents of this policy and The Regulation.

YOUR RIGHTS UNDER THE DATA PROTECTION RULES

The Regulation gives you (and anyone else about whom personal data is held) specific rights in relation to the information that is held about you. The GDPR introduces a right for individuals to have personal data erased (*'the right to be forgotten').* Some of these rights are summarised below.

Under The Regulation, you are able to:

- Obtain confirmation that First Light holds personal information about you, as well as a written description of the information, the purposes for which it is being used, the sources of the information and the details of any recipients
- Obtain access to the personal information, which is held about you
- Rectify any inaccurate data held without delay
- Request that personal data be removed/deleted where no compelling reason exists to continue processing such data
- Restrict the processing of personal data under certain circumstances as laid down in The Regulation
- Object to the processing of personal data where First Light does not have compelling legitimate grounds as laid down in The Regulation

- It is important to note that this is not an absolute right to review all the information that is held about you, as there are various exceptions to this right contained in The Regulation. These include:

  (a) where personal data is kept for the purpose of preventing, detecting or investigating offences and related matters; and
  (b) where the data is an expression of opinion about you given by another person in confidence.

YOUR RESPONSIBILITIES UNDER THE DATA PROTECTION RULES

As well as having rights under The Regulation, all employees when processing personal data must comply with the general data protection rules set out in this Policy. Failure to comply with the rules and requirements in relation to data protection may result in disciplinary action being taken against you.

YOUR PERSONAL INFORMATION

First Light requires certain personnel information which may include but is not limited to the below list. In order to assist First Light in ensuring that your personal information is kept up to date, you should inform the CEO of any changes as they arise;

- CV / Application form
- Qualifications/ Education
- Address and other contact details
- Emergency contact name and number
- Bank account details
- Attendance records
- Health and Safety documentation

PERSONAL INFORMATION RELATING TO EMPLOYEES AND CLIENTS

- If as part of your job, you hold any personal information about other employees of First Light, clients or about anyone else, then you also need to take steps to ensure that you are following the guidelines set out below. Please note that the following guidelines apply equally to documents containing personal information, which are kept in files, as well as information, which is kept electronically

- You should not keep personal information about people, which you no longer need, or which is out of date or inaccurate. You should therefore review any personal information that you hold annually, bearing these principles in mind
- All personal information must be kept securely and should remain confidential
- If you receive a request from someone to give them any personal data about an employee or other individual you should refer them to the CEO. If the request relates to a client, you should refer them to First Light's Clinical Director. First Light needs to verify the identity of the person making such a request and has to balance various considerations when deciding whether and how to respond to such request, including compliance with The Regulation. It is therefore important to refer such requests to the CEO or the Clinical Director, as appropriate, so that s/he can ensure First Light's obligations are complied with
- Accessing, disclosing or otherwise using employee records or other personal data without authority will be treated as a serious disciplinary offence and may result in disciplinary action being taken in accordance with First Light's disciplinary procedure up to and including dismissal

If you are unsure about the application of these guidelines to the information you hold as part of your job, you should contact the CEO for further guidance.

BREACH

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, First Light shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to Management.

VARIATION

First Light may issue further guidance or make amendments to this Policy from time to time, which will be notified to you.