First Light

Data Protection Act Policy

Document Control	
Supersedes	Supersedes: Version 4.0 Significant changes: Update name
Originator or modifier	Originated By: Business Manager
Ratification	Referred For Approval By: Board Members Date of Referral: July 2017
Application	All paid staff and volunteers
Circulation	Issue Date: November 2014 Circulated By: Placed in shared drive

First Light
Metropolitan House
The Millfields
Plymouth PL1 3JB

CONTENTS

1. Introduction

The regulations set out in this document are set down by The Board of Trustee and the Chief Executive of First Light. The compliance frameworks on the data protection and privacy criteria, forms part of First Light policy and compliance regulations, to clients, employees and associated personnel of First Light.

Clients are entitled to protection of their privacy, as are staff and others who might have dealings with Twelve Company. Privacy considerations normally apply to a great deal of information that First Light may hold about clients and staff that may include a mix of personal data (address, age, treatment status, evaluation and assessment and personal welfare (family matters, medical matters, financial matters and so on).

Twelve's staff may require access at times to personal information about clients. To the extent that the information is private First Light will restrict access to those staff that may need the information in order to carry out their responsibilities in the personal and/or interests of the clients.

The Data Protection Act applies to internally but also externally. For example at MARAC meetings, Child Protection meetings etc.

2. Policy Statement

High-profile security breaches have increased public concern about the handling of personal information. As some 80% of security incidents involve staff there is a clear need for all workers to have a basic understanding of the Data Protection Act 1998 (the Act).

This Policy outlines some of the practical implications of the Act and is intended as a basic training framework for all staff and volunteers.

First Light is registered with the Information Commissioners Office and requires all staff, both employed and volunteers, to be aware of the responsibilities placed on the organisation by the Data Protection Act 1988.

3. Policy Standards

Data protection laws affect how businesses and other organisations are allowed to make use of personal information. They must follow these rules if they store or process people's details - i.e. keeps client or employee records.

This guide explains the requirements of the Data Protection Act 1998 and outlines steps your organisation can take to ensure they meet them which involves notifying the Information

Commissioner's Office (ICO) about the personal information your business holds and what it's used for.

There is specific guidance on what should be considered if involved in recruiting staff and managing employee records, as well the rules on monitoring workers. This guide contains advice on areas of good practice for staff to ensure they understand the implications of the Act.

4. Eligibility and Scope

All members of staff/volunteers who record and/or process personal data in any form must ensure that they are working within the requirements of the 1998 Act, that they comply at all times with the Data Protection Principles and with the institutional regulations and procedures set out in this document and in any supplementary procedures which may be introduced from time to time. Whilst the 1998 Act places certain responsibilities on First Light and individual members of staff who control the contents of and/or process personal data are personally responsible for complying with the 1998 Act.

This policy should be read in conjunction with the following Policies and Procedures set out by First Light:

1. Standard Framework for Record Keeping and Information Sharing
2. Confidentiality Policy

Failure to act in line with this policy will be treated as a disciplinary matter and could lead to termination of employment under Gross Misconduct.

4. What does the Data Protection Act 1998 apply to

The Data Protection Act 1998 applies to personal information.

That is either held in a form in which it can be or is being processed automatically (this would in the main be on computer) or within a structured manual filing system. Statements of fact and expressions of opinion about an individual data subject are personal.

This is data about living, identified or identifiable individuals and includes information such as names and addresses, bank details, and opinions expressed about an individual.

What are the main requirements?

The Act regulates how personal information is used and requires organisations to comply with eight principles or rules of good information handling.

Personal information can be used by an organisation only where it meets one of six conditions set out in the Act. In most cases, it should not be too difficult to meet one of these conditions, which include having the individual's consent or having a legitimate interest in using their personal information.

Sensitive personal data

The Act classifies some personal information as 'sensitive' and there are stricter rules about this. This is information about:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- trade union membership
- physical or mental health condition
- sexual life
- offences or alleged offences committed
- proceedings relating to those offences or alleged offences

You can only use sensitive personal information where you can meet at least one of a narrower set of conditions - as well as being able to meet one of the six standard conditions - for processing personal information. These narrower conditions make sure that this sensitive information is only used where there is an essential need for an organisation to use it.

The eight data protection principles

All staff in First Light will comply with the data protection principles which are set out in the Data Protection Act 1998. In summary these state that personal data shall:

i. Be obtained and processed lawfully and shall not be processed unless certain conditions are met.

ii. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.

iii. Be adequate, relevant and not excessive for those purposes.

iv. Be accurate and kept up to date.

v. Not be kept for longer than is necessary for that purpose.

vi. Be processed in accordance with the data subject's rights.

vii. Be kept safe from unauthorised access, accidental loss or destruction.

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

Data security

First Light has appropriate security measures in place to protect personal information against unlawful or unauthorised use or disclosure. Staff must adhere to these.

Individuals' rights under the Data Protection Act 1998

The Data Protection Act 1998 gives individuals certain rights in relation to the use of their personal data. These rights are as follows:

- **The right of subject access** - gives individuals the right to obtain information held about themselves.
- **The right to prevent direct marketing** - individuals can ask you at any time not to use their personal information for direct marketing purposes. An individual must put their request in writing and you must act on the request in a reasonable period of time. In most cases, this should be within 28 days.
- **The right to have personal information corrected** - an individual has the right to have incorrect or misleading personal information held about them corrected. If you don't do this, the individual could obtain a court order directing you to correct, delete, block or destroy the information. If this happens, it will be up to the court to decide if the information is inaccurate and what (if anything) to do about it. The individual may also ask the court for compensation and costs.
- **The right to prevent automated decisions** - this allows individuals to stop important decisions about them being made by solely automated means - for example, decisions made only by a computer. This can include recruitment decisions made solely on the basis of psychometric testing. There are some automated decisions which, under certain circumstances, are exempt from this right. A sensible course of action is to allow the individual the right to appeal a decision taken in this way.

Personal information access rights

The Data Protection Act 1998 gives individuals the right to access the personal information you process about them.

Individuals have the right to:

- know whether you, or someone else on your behalf, is processing personal information about them
- know what information is being processed, why it is being processed and who it may be disclosed to
- receive a copy of the personal information about them
- know about the sources of the information

To obtain access to personal information held about them, an individual must send either a written or electronic request - known as a **subject access request** (SAR). The SAR doesn't have to refer to the Act but should make it clear that it is a formal request from the individual and not just an everyday enquiry. A fee of up to £10 can be charged to provide the information requested.

If you are not sure about the identity of an individual requesting information, you should ask for proof. This could be an official document, such as a council tax bill, driving licence or passport.

You can request additional information that you might need to respond to the SAR. For example, if an individual has requested emails you could ask when the emails were sent, or for the senders or recipients of the emails.

First Light must respond to a SAR no later than 40 days after receiving it.

The 40-day period does not start until you receive any additional information you need. First Light doesn't need to supply the information until after receiving any fee payable.

First Light must provide the information requested in a permanent format - such as a computer printout, letter or form - unless the individual agrees otherwise, it is not possible to supply such a copy or you can show that it will involve 'disproportionate effort'. If this is the case, you must still provide access to the information in another way.

First Light must ensure that the information can be understood. For example, if there are any codes used, explain what they mean.

Why comply with a SAR?

First Light can be fined heavily for breaking data protection rules but complying with a SAR also has other business benefits, including:

- reducing correspondence being sent using out-of-date information or to incorrect addresses, and so potentially saving time and money
- increasing client confidence in your information

- reducing the risk of a complaint being made against First Light
- protecting First Light against compensation claims

Staff attitudes to data privacy and security

- Data privacy and security are a key part of data protection rules, so staff need to be aware of their importance. For example, the loss or theft of a USB stick or laptop containing personal information about customers could seriously damage your business' reputation, as well as lead to severe financial penalties. It is therefore a requirement that all equipment is encrypted that holds any personal information.

Data protection for employee records and when recruiting

The Data Protection Act applies to personal information First Light holds about **all** individuals - not just clients. This is adhered to when recruiting new staff and storing employment records.

People can claim compensation if they suffer as a result of the business breaking data protection rules.

Key considerations during recruitment

To comply with the Data Protection Act when recruiting staff, we shall:

- give the business name and contact details on all job adverts.
- not collect more personal information than we need - eg bank details are only necessary from the successful candidate and motoring offences are only relevant if driving is a part of the job
- only ask about criminal convictions if this is justified by the job type
- not ask about 'spent' convictions unless the job is covered by the Exceptions Order to the Rehabilitation of Offenders Act 1974
- keep any personal information we obtain as secure as possible
- only record whether a criminal records check is satisfactory/unsatisfactory and not hold on to detailed information
- use the information we collect for recruitment purposes only - if we plan to use it for another purpose, eg for a marketing mailing list, we must explain so clearly
- only keep information obtained though recruitment for as long as we have a clear business need for it and then dispose of it securely - eg by shredding

Key considerations for employee records

All staff, associates/affiliates and consultants are entitled to protection of their privacy. Privacy considerations normally apply to some information that First Light may hold about its staff and may include a mix of personal data (address, qualifications, performance indicators, emergency contact details inclusive of family members, medical details and financial data).

Staff in a line management role may require access at times to personal information about staff to ensure that performance management processes are effective and that they have access to emergency contact information in the case of a crisis. To the extent that the information is private, we will restrict access to those staff who may need the information in order to carry out their responsibilities in the business and operational interests of First Light except where they conflict with any UK or European legislation.

Other than to confirm that individuals are, or have been, a staff member of associated/affiliated with First Light, First Light undertakes not to disclose personal information about its staff and its associates/affiliates, to people outside of First Light (other than in accordance with any legal or commercial obligations as determined by First Light or to staff who have no need of access to the information (inclusive of consultants/contractors), unless staff and associates/affiliates advise First Light in writing, that they have given permission.

To manage all employee records as responsibly as possible under the Data Protection Act. We shall:

- keep records secure - eg by locking paper records in a filing cabinet and using passwords to protect computerised ones or store in limited access shared drives.
- ensure only appropriate, authorised staff with the necessary training have access to employment records
- store sensitive information separately – e.g. don't give managers access to employees' sickness records when a simple record of absences is sufficient
- don't keep records that are irrelevant, excessive or out of date
- periodically let staff check and update information in their own records
- not give a reference about a worker or an ex staff member without first checking that they are happy for you to do so

- ensure records are disposed of securely – e.g. by shredding - once you no longer have a business need or legal requirement to keep them

Giving staff access to records

Your workers have a legal right to ask for a copy of information you hold about them. This includes information about grievance and disciplinary issues, and information you obtain through monitoring.

However, you can withhold information where giving it to the worker would make it more difficult to detect a crime.

You may also need to withhold information if it concerns a third party. For example, if a worker has been accused of harassment, you may need to protect the identity of the person making the accusation.

A worker may object to you holding or using information about them if it causes them distress or harm. If so, you should delete that information or stop using it in the way complained about, unless you have a compelling reason not to.

The issues covered on this page are covered in much greater detail in the Employment Practices Code published by the Information Commissioner's Office (ICO).

Monitoring workers

The Data Protection Act 1998 covers personal information processed about the monitoring of workers, including casual, contract and agency staff.

Monitoring involves activities that set out to collect information about workers by keeping them under some sort of observation. This could include monitoring electronic communications, video and audio and using information from others.

The Information Commissioner's Office (ICO) has developed a code of best practice to help businesses comply with the Act. Part 3 of the Employment Practices Code states that any adverse impact of monitoring on workers must be justified by the benefits to employers and others.

To help employers establish whether they are justified in monitoring, the code outlines an **impact assessment** which involves:

- identifying the purpose behind the monitoring
- identifying any adverse impact of the monitoring on the subjects of the monitoring
- considering alternatives to monitoring

- taking account of obligations that arise from monitoring, such as setting up new processes to ensure records are secure

The code states that workers should be made aware of the nature, extent and reasons for monitoring, unless covert monitoring is justified. If you are monitoring workers to enforce the rules and standards of your business, these should be set out in a policy that also refers to the nature and extent of any associated monitoring.

Covert monitoring will rarely be justified - you must be satisfied that there are clear grounds for suspecting criminal activity or other malpractice. A reliable test to use would be whether the activities you wish to monitor are sufficiently serious to involve the police, although you would not actually have to involve them.

You must make sure that those responsible for monitoring in your business are aware of the Data Protection Act 1998 and its implications. Keep the number of workers who have access to personal information obtained through monitoring to a minimum.

If information gathered through monitoring is to have consequences for a member of staff, that worker should first be given the chance to give their side of the story. It could be that the information obtained is misleading or inaccurate.

Bogus agencies

Businesses throughout the UK continue to be troubled by bogus data protection notification agencies. The ICO is the only statutory authority for administering and enforcing the public register of data controllers.

The Information Commissioner's Office

The Information Commissioner's Office (ICO) is an independent public body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. One of the ICO's responsibilities is enforcing the Data Protection Act 1998.

The ICO promotes good practice by:

- publishing guidance to simplify compliance
- running a helpline
- encouraging the development of codes of practice
- taking enforcement action where necessary
- seeking to influence national and international bodies on privacy and access matters

- maintaining a register of organisations and businesses that process personal information

5. Good Practice Guidelines

5.1 Keeping personal information secure

- Keep passwords secure – change regularly, no sharing
- Lock / log off computers when away from desks
- Dispose of confidential paper waste securely by shredding
- Prevent virus attacks by taking care when opening emails and attachments or visiting new websites
- Work on a 'clear desk' basis - securely store hard copy personal information when it is not being used
- Visitors should be signed in and out of the premises, or accompanied in areas normally restricted to staff
- Position computer screens away from windows to prevent accidental disclosures of personal information?
- Encrypt personal information that is being taken out of the office if it would cause damage or distress if lost or stolen
- Keep back-ups of information

5.2 Meeting the reasonable expectations of clients and employees

- Collect only the personal information we need for a particular business purpose
- Explain new or changed business purposes to clients and employees, and obtain consent or provide an opt-out where appropriate
- Update records promptly – for example, changes of address, contact preferences
- Delete personal information the business no longer requires
- We are committing an offence if we release client / employee records without consent

5.3 Disclosing customer personal information over the telephone

- Be aware that there are people who will try and trick you to give out personal information
- To prevent disclosures you should carry out identity checks before giving out personal information to someone making an incoming call
- Perform similar checks when making outgoing calls
- Limit the amount of personal information given out over the telephone and to follow up with written confirmation if necessary

5.4 **Notifying under the Data Protection Act**

- Ensure First Light has a notification entry with the ICO
- Monitor changes in business use of personal information, and notify the ICO if appropriate

5.5 **Handling requests from individuals for their personal information (subject access requests)**

- People have a right to have a copy of the personal information the organisation holds
- Recognise a subject access request
- Forward it to the appropriate person
- Company has a maximum of 40 days to respond
- The maximum fee that can be charged is £10
- Check the identity of the requester