|  |
| --- |
| **EXPECT GROUP OF COMPANIES** |
| DATA PROTECTION, INFORMATION and ‘IT’ MANAGEMENT |
| **Scope**This document describes staff and Expects responsibility to comply with the General Data Protection Regulations 2018 (GDPR) and Data Protection Act (Amended 2018). |
| **Related Documents**MA004 Confidentiality QG001 Record Keeping GuidelineQMP015 Information Sharing Policy |
| CONTENTS[1 AIM 2](#_Toc29384155)[2 STANDARDS OF EXCELLENCE 2](#_Toc29384156)[3 THE DATA PROTECTION ACT 2018 AND GDPR 2018 2](#_Toc29384157)[4 MANAGEMENT OF COMPANY COMPUTER SYSTEMS 4](#_Toc29384158)[5 STAFF OBLIGATIONS 5](#_Toc29384159)[6 DATA SECURITY 6](#_Toc29384160)[7 SERVICE USER RIGHTS 7](#_Toc29384161)[8 TRAINING 8](#_Toc29384162) |
| **Issue Status** |
| **First Issued:** | 18 June 2007 | **Current Issue Date:** | 8 January 2020 |
| **Annual Review Record** |
| 1st Review by: | Date of Review | 2nd Review by: | Date of Review | 3rd Review by: | Date of Review |
|  |  |  |  |  |  |
| 4th Review by: | Date of Review | 5th Review by: | Date of Review | 6th Review by: | Date of Review |
|  |  |  |  |  |  |
| Author/Owner: | Robert MacDonald | Designation: | Service Manager, Policy |
| Approved by: | Steve McDermott | Designation: | Chief Executive Officer |
| Signed: Chief Executive Officer |

EXPECT GROUP OF COMPANIES

DATA PROTECTION, INFORMATION AND ‘IT’ MANAGEMENT

# AIM

* Records required by regulation for the protection of the Service Users and for the effective running of the service, are maintained, up to date and accurate.
* All employees observe the provisions laid down in the GDPR and Data Protection Act 2018 and any subsequent re-enactment or modification thereof.

# STANDARDS OF EXCELLENCE

* The Company will provide any training/education necessary to comply with relevant legislation.
* Service Users have an “enforceable right” to access the information kept about them by the Company.
* Each employee's knows their responsibility to ensure that they are fully aware of and understand the terms of the legislation.
* Personal Information covers not only Service Users but extends to individual staff files.
* Under the **Data Protection Act 2018,** the organisation has a nominated user/data controller, this is currently the Service Manager for Policy and IT.

# THE DATA PROTECTION ACT 2018 AND GDPR 2018

## The Act is concerned with the automatic processing of information about living individuals (personal data) and gives rights to the individual who is the subject of that information. The legislation places certain obligations on The Company in respect of information it processes or causes to be processed on its behalf by a third party.

## The aims of the Act are embodied in the eight Data Protection Principles, which are as follows:

### The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.

### Personal data shall be held only for one or more specified and lawful purpose.

### Personal data held for any purpose/s shall not be used or disclosed in any manner incompatible with such purpose/s.

### Personal data held for any purpose/s shall be adequate, relevant and not excessive to that purpose/s.

### Personal data shall be accurate and, where necessary, kept up to date.

### Personal data held for any purpose/s shall not be kept for longer than is necessary for such purpose/s.

### An individual shall be entitled at reasonable intervals and without undue delay or expense to:

1. be informed by any data user whether she/he holds personal data of which the individual is the subject.
2. provide access to any such data held.
3. where appropriate, have such data corrected or erased.

### The data user shall take appropriate security measures against:

1. unauthorised access, alteration, disclosure or destruction of personal data.
2. accidental loss or destruction of personal data.

## The most significant requirement of the Act is that all data users (whether companies or individuals) must register with the Data Protection Registrar unless covered by the exclusions in the Act.

## The Company must complete a registration covering all personal data presently held, specifying:

1. the purposes for which the data is used.
2. a description of the data and the data subjects.
3. the sources and disclosures applicable to the information comprising the data.
4. the countries outside the UK to which the data is transferred (overseas transfers).

## The initial registration has to be updated as and when changes occur in any of the above details. The holding and processing of unregistered data, which is covered by the Act, is a criminal offence and subject to unlimited fines. Therefore the Company must operate within the terms of its registration.

3.6 It is important that all employees are aware of the existence of this Act and the principles on which it is based. In particular they must:

 a) not access, process or disclose any personal data other than is necessary, within the terms of the Company's registration, to carry out the role for which they are employed.

 b) understand that any change in purposes, description, sources, disclosures, overseas transfers of the personal data under their control may require an amendment to the Company's registration.

# Management of company computer systemS

## The ‘IT’ Manager will ensure, all staff required to access the Company’s computer systems are issued with a ‘Username’ and ‘Password’.

## Passwords must:

* be at least 12 characters long;
* contain at least one number;
* contain a mixture of lowercase and at least 1 capital letter;
* contain at least one non-alphanumeric character e.g.: \* £ $ %.

## To access the Company’s computer and email systems, a user will be required to input a valid user name and password.

## The IT Manager will ensure each member of staff is allocated a “security group”, when their account is set up. This will ensure only authorised persons have access to Directories and data relevant to their role. The Company directory structure is designed to give maximum security for data protection purposes.

## The IT Manager will set up a Company email account for all new staff. Non office based staff will be granted access to their email account only. The Company network and emails are independent of each other.

## All office based staff must ensure that any personal data relating to Service Users or staff is secured and where possible encrypted using the software’s built in encryption tools.

## All staff will be given secure access to the Company intranet via the Company web page. The Company intranet will form a repository for the storage of non-sensitive information e.g. procedures, forms, information booklets and other relevant information.

# Staff obligations

## In connection with their own personal data, all staff should:

* ensure that any information that they provide to the Company in connection with their employment is accurate and up to date.
* inform the Company of any changes for which they are responsible, for example, changes of address (the Company cannot be held accountable for errors arising from changes about which it has not been informed).

# Data Security

## All staff must:

* ensure that any personal and or sensitive data which they hold is kept securely
* ensure that personal information and or sensitive data is not disclosed either orally or in writing, intentionally or otherwise to any unauthorised third party.
* remember that unauthorised disclosure may be a disciplinary matter, and could be considered gross misconduct in certain cases.
* make reasonable efforts to ensure that all personal information is kept securely, but should pay particular attention to the security of sensitive data. All personal data should be accessible only by those who need to use it and sensitive data must be either kept in a lockable room with controlled access, *or*:
1. kept in a locked filing cabinet, *or*
2. in a locked drawer, *or*
3. if computerised, be password protected.

## While the security of the computer network is the responsibility of the Company's senior managers, staff must take appropriate security precautions in respect of day-to-day PC usage. Care must be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. Screens should not be left unattended when personal data is being processed and manual records should not be left where they can be accessed by unauthorised staff. When manual records are no longer required, they should be shredded and disposed of securely; and the hard drives of redundant PCs must be wiped clean.

## Off-site use of personal data presents a potentially greater risk of loss, theft or damage to personal data; and the institutional and personal liability that may accrue from the off-site use of personal data is similarly increased. Staff should take particular care when laptop computers or personal machines are used to process personal data at home or in other locations outside the Company; and staff should also be aware that this document and their responsibilities under it apply when data is processed under such circumstances.

## It is a condition of employment that staff consent to the processing of their personal data. Nonetheless, it is recognised that there might be occasions when a member of staff or student has good reason for wishing details in certain of these lists or categories to remain confidential or to be restricted to internal access, in which case they should contact the IT Manager, who acts as the designated data controller. It is understood that this is especially the case in connection with the publication of photographic images of staff, particularly on web pages; all members of staff are advised that such images should not be made publicly accessible without the consent of the individuals concerned.

# SERVICE USER RIGHTS

## As part of the support that the Company offer to Service Users, the Company need to collect personal information about them. This information will not be shared with other people apart from the staff where they live or within the Company.

## Service Users have the right to:

* see the information that the Company keep about them.
* disagree with the information.
* have this information corrected if it is wrong.
* have the information written in their personal file.
* have all information kept up to date.
* have this information stored securely.

## If the Service User decides that they no longer want the Company to provide their support, then the law says the Company must keep all the information we have gathered about them for a minimum of 3 years from the date of last entry.

# Training

## All new staff shall be made aware of their responsibilities around data protection and on confidentiality as part of their induction process. Existing staff will be offered training to National Training Organisation standards covering basic information about confidentiality, data protection and access to records. Training in the correct method for entering information in Service Users' records should be given to all care staff. The nominated data user/ data controller for the Company should be trained appropriately in the **Data Protection Act 2018.** All staff who need to use the computer system must be thoroughly trained in its use.