SJMT people at heart	**Data Protection and Confidentiality Policy** **HR-POL-11** **Version: 04**
Date: April 2022	**Developed by:** CEO
Review period: 3 years	**Owned by:** Board of Trustees
Review date: April 2025	**Authorised by:** Board of Trustees

1. POLICY STATEMENT

1.1 Everyone working for or on behalf of the Trust has a duty to keep information about residents, carers, clients, staff and other individuals confidential and secure, and to protect the privacy of information about individuals. This duty is enshrined in law and in professional codes of conduct.

1.2 It is the policy of the Trust that the measures outlined in this policy should be followed by all employees, Trustees, volunteers and contractors in order that compliance with legislation and good practice can be maintained.

2. INTRODUCTION

2.1 This document is a statement of Trust policy on Data Protection and Confidentiality. It includes guidance for staff on processing information in accordance with current legal obligations and best practice.

2.2 The Trust needs to collect and use information about people with whom it deals in order to operate. These include current, past and prospective clients, current, past and prospective employees/volunteers, suppliers, clients/customers, donors/fundraisers and others with whom it communicates. In addition, it may occasionally be required by law to collect and process certain types of information to comply with the requirements of Government departments for business data.

2.3 For the purposes of this policy, the terms ‘data’ and ‘information’ are used interchangeably.

3. CONTEXT

3.1 The Data Protection Act (1998) defines a legal basis for the handling in the UK of information relating to living people. The General Data Protection Regulation, in force in the UK from 25 May 2018, updates the Data Protection Act and introduces new requirements for public authorities who handle personal data.

4. PURPOSE

The purpose of this policy is:

- To ensure any personal information collected and held by the Trust is processed fairly and lawfully.
- To promote best practice in the processing of personal information.

- To ensure that Trust staff involved in processing personal information understand their responsibilities and obligations.
- To ensure that Trust staff responsible for the processing of personal information are adequately trained to fulfil their responsibilities and obligations.
- To outline the procedure for reporting and investigation of a suspected breach of Confidentiality and/or Data Protection.
- To provide assurance to our clients, staff and others with whom we deal that their personal information is processed lawfully and correctly and held securely at all times.

5. SCOPE

5.1 This policy relates to all types of information within the Trust. These include:

- Client/resident information
- Personnel information
- Organisational information.

5.2 This policy covers all aspects of information, including (but not limited to):

- Storage, filing and record systems - paper and electronic
- Transmission of information – e-mail, post, telephone and fax
- Images, including CCTV and photographs

5.3 This policy applies to:

- All information systems purchased, developed and managed by, or on behalf of, the Trust.
- All Trust employees (including those on fixed term contracts), Trustees, contractors, donors, fundraisers and volunteers.
- Members of other organisations granted temporary or permanent access (for example to undertake audits or inspections) to confidential information held by the Trust.
- All systems provided by Third Party contractors, where the service has been negotiated on the Trust's behalf e.g. funders.

6. DUTIES

6.1 Chief Executive

The Chief Executive has overall responsibility for Information Governance which includes the Data Protection Act 1998. As the Accounting Officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

6.2 Chair

The Chair has Board level responsibility for the management of information risk within the Trust and the development and maintenance of Information Governance practices throughout the Trust including business continuity measures to ensure the safety and availability of information assets.

6.3 The Board of Trustees

The Board is responsible for ensuring that the Trust establishes, monitors and maintains appropriate systems, processes and reporting arrangements for the management of all aspects of information governance, data protection and confidentiality. It supports and drives the broader information governance agenda and provides assurance that effective information governance best practice mechanisms are in place within the Trust.

6.4 Head of Central Services

The Head of Central Services is responsible for the operational day to day management of all issues relating to Information Governance, including drafting policy documents, procedural guidance, training, audit and dealing with all IG related queries.

6.5 Director of Operations

The Director of Operations holds the role of Caldicott Guardian for the Trust. This role relates specifically to the medical and health and social care data held across the Trusts care services. The Director of Operations will work with the Head of Central Services to ensure that any matters related to data of this nature will be looked at within the realms of Information Governance as well as the Caldicott principles.

6.6 All staff

6.6.1 It is the responsibility of each member of Trust staff to familiarise themselves with, and follow the policies relevant to their role/work.

6.6.2 All Trust staff, whether operational or administrative, have responsibility for the safety and proper management of the information they process, and for the prompt reporting of any Information Governance incident using the Report a Personal Data Breach Form. This form must be completed at Head Office and handed to the Head of Central Services for further action.

6.6.3 All staff must complete their Information Governance refresher training annually.

6.6.4 All offices must display the Data enquiry flow chart as an easy reference guide to ensure that the correct procedures are followed.

6.7 Managers

Managers should ensure through appraisal and regular supervision that staff are aware of and comply with key policies and procedures relevant to their work.

7. DEFINITIONS

Personal data: Is information that could be used in isolation or in combination with other items of information to identify a data subject directly or indirectly. It includes such items of data as: Name, address, postcode, NHS number, National Insurance Number, family, lifestyle or social circumstances, education and training details, employment details, financial details, photographs and other images.

Special categories of personal data: Any of the following data held by the Trust are considered to be special categories of personal data under the GDPR, and additional safeguards apply to processing these data: Racial or ethnic origin, Political opinions, Religious or other beliefs, Trade union membership, Physical or Mental Health, Sexual life, Genetic data, Biometric data, Personal

data regarding criminal convictions and offences are not included, but similar safeguards apply to processing these data.

Processing: Any of the following actions, in relation to the data, constitute processing: - Obtaining, Accessing, Recording, Retrieval, Consultation, Holding, Disclosing, Sharing, Using, Transmission, Erasure, Destruction.

Data Subject: Data Subject means an individual who is the subject of the personal data, either directly or can be identified from it. A data subject must be a living individual.

Data Controller: The Data Controller is the individual, company or organisation that determines the purpose and the manner in which personal data may be processed. Sir Josiah Mason Trust is the Data Controller for the purposes of the Act.

Data Processor: Data Processor, in relation to personal data, means any other person other than an employee of the Trust who processes data on behalf of the Trust.
Recipient: Recipient, in relation to personal data, means any person to whom data are disclosed (including employees or agents of the Trust).

Third Party: Third party, means any person other than: the data subject, the data controller, any processor or other person authorised to process for the data controller

Data protection legislation: Within this policy, 'data protection legislation' shall be taken to mean the General Data Protection Regulation, the Data Protection Act 1998, or any subsequent UK legislation.

Organisational information: Organisational information means information other than personal information, (such as financial or business planning information, or minutes of confidential meetings) which may have a commercial value or which, if disclosed inappropriately, may disadvantage the Trust.

Information Commissioner: formerly known as the Data Protection Commissioner.

Notification: formerly known as Registration.

Caldicott Guardian: A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly.

8. OWNERSHIP AND CONSULTATION

The Chief Executive is the author and owner of this policy. The Board of Trustees have been consulted during the drafting of this policy.

9. REVIEW

This policy will be reviewed every 3 years, subject to changes in legislation, advances in technology or the production of national/regional guidance.

10. PROCESS FOR MONITORING COMPLIANCE

10.1 A quarterly report will be submitted to the Finance and Performance Board. This report will include information on data protection performance and confidentiality breaches.

10.2 Electronic client record systems will be subject to periodic audit to detect inappropriate access to confidential records. Audits will be undertaken or commissioned to assess wider information and IT security arrangements.

10.3 Managers will also monitor compliance within their work area, and take appropriate action when infringements of this policy are brought to their attention.

11. TRAINING

11.1 Guidance on confidentiality and data protection will be produced and delivered to all staff as required.

11.2 Training needs will be assessed by the HR Department and appropriate training provided. Such training will normally be through e-learning packages. All new staff will receive Information Governance awareness training as part of their corporate induction. Information Governance refresher training, also including data protection and confidentiality, will be a requirement for all existing staff, and will form part of the Trust's suite of statutory and mandatory training.

11.3 Staff employment contracts will contain information highlighting individual responsibilities in respect of data protection and confidentiality. Examples of these clauses are shown in Appendix 1 of this policy.

12. POLICY PRINCIPLES

12.1 This Policy is underpinned by the 8 Data Protection Principles under the Data Protection Act 1998 as retained under the GDPR.

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

12.2 Legal requirements exist in relation to the collection, storage, accuracy, retention and disclosure of personal information. All processing of information by Trust staff must be carried out in accordance with principles set out in the Data Protection Act and any amending legislation, and with other relevant guidance.

12.3 While Data Protection legislation applies to living individuals, where possible the same level of confidentiality should be provided to the records and information relating to a deceased person as one who is alive.

12.4 Individuals have certain rights regarding their personal data. These include:

- the right to be informed
- the right of subject access
- the right to rectification
- the right to erasure (to be forgotten)
- the right to restrict processing
- the right to data portability
- the right to object
- the right not to be subject to automated data processing

The Trust will ensure that procedures are in place to enable individuals to take advantage of all applicable rights regarding their personal data.

12.5 In addition to their rights under data protection legislation, individuals have a legal right to respect for private and family life under the Human Rights Act 1998. Staff must respect the dignity and right to confidentiality of clients when collecting and processing personal data. This includes the use of photographs and images, and the taking and sharing of images relating to clients for non-professional purposes is not permitted.

12.6 The Trust will undertake Data Protection Impact Assessments (DPIAs) if this is required, to further its intention of achieving data protection by design and by default. The Director of Operations and Head of Central Services will determine whether a Data Protection Impact Assessment is required for eligible activities that fall outside of current processing activities using the ICO guidance and screening checklist.

12.7 The Trust will process personal data and special categories of personal data only where there is a valid legal basis for doing so under GDPR or any equivalent UK legislation. Where special categories of personal data are processed for some specific purposes as set out under GDPR or any equivalent UK legislation, the Trust will where relevant produce and retain appropriate policy documents setting out in relation to that processing the Trust's processes for maintaining compliance with the conditions for processing, and the retention periods applicable to that data.

12.8 The Trust will maintain a record of its processing activities, in a format which complies with requirements set out in GDPR or any equivalent UK legislation. This includes having an Information Asset register (IAR) which records what information we have, where we keep it and how it is protected. Further to this the Trust also has a Record of Processing Activities (ROPA) which records where the Trust receives data and where data is sent to and what legal basis this is for. These records are held centrally and monitored annually by the Head of Central Services.

12.9 This policy is further guided by the 7 Caldicott Guardian Principles.

These 7 Caldicott principles are:

Principle 1: Justify the purpose for using confidential information

Every proposed use or transfer of personally identifiable information, either within or from an organisation, should be clearly defined and scrutinised. Its continuing uses should be regularly reviewed by an appropriate guardian.

Principle 2: Don't use personal confidential data unless absolutely necessary

Identifiable information should not be used unless it's essential for the specified purposes. The need for this information should be considered at each stage of the process.

Principle 3: Use the minimum necessary personal confidential data

Where the use of personally identifiable information is essential, each individual item should be considered and justified. This is so the minimum amount of data is shared and the likelihood of identifiability is minimal.

Principle 4: Access to personal confidential data should be on a strict need-to-know basis

Only those who need access to personal confidential data should have access to it. They should also only have access to the data items that they need.

Principle 5: Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personally identifiable information are aware of their responsibilities and their obligation to respect patient and client confidentiality.

Principle 6: Understand and comply with the law

Every use of personally identifiable data must be lawful. Organisations that handle confidential data must have someone responsible for ensuring that the organisation complies with legal requirements.

Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients and within the framework set out by these principles. They

should also be supported by the policies of their employers, regulators, and professional bodies.

13. TRANSFER OF PERSONAL DATA

13.1 Any transfer of personal data must be carried out securely with an adequate level of protection given to the data in transit in accordance with our IT Security policy. This applies both to the transfer of paper-based information, as well as to data transferred via electronic means, (including email and portable devices such as memory sticks). The Trust's IT Security Policy provides guidance on the secure transmission of personal data. It is recommended that users contact the Finance department before considering the transmission of any significant amounts of personal data to ensure they are using the most appropriate and secure mechanism.

13.2 No personal data may be transferred outside the UK or the European Union without the agreement of the Head of Central Services. Transfers of personal data outside the EU or UK will take place only where the Trust receives assurance that an equivalent level of data protection applies in the receiving country as that provided in the UK. Safeguards must be in place to ensure that personal data is handled, stored and transmitted securely, regardless of the destination.

13.3 Advice should be sought from the Head of Central Services before transferring any personal data for the first time, regardless of the destination.

14. ACCESS TO AND DISCLOSURE OF PERSONAL INFORMATION

14.1 Care must be taken to ensure any access to or disclosure of personal or sensitive information is for an authorised purpose. Anyone in doubt as to whether a disclosure of information is authorised should check with their manager. Care services staff should consult with the Caldicott Guardian on matters of Health and social care data.

14.2 Data subjects will have a right of access to their information. Requests from clients or their representatives to see all personal data held on them, including e-mails and computer or paper files must be made in writing to the Head of Central Services. The Data Processor (Sir Josiah Mason Trust) must comply with such requests within 30 days of receipt of the written request.

14.3 No information relating to clients should be given over the telephone unless the person communicating the information is sure that the person they are speaking to is entitled to receive the information (e.g. a GP Practice).

14.4 Personal information will usually be disclosed only if the individual has given their consent to the disclosure. However, under certain circumstances, the Trust has a power or an obligation to disclose personal information without the individual's consent, (for example to assist the police in preventing or detecting crime, or where a court order is produced). Where the Trust has a power to disclose information without consent, that power will be exercised only if members of the public, patients or staff are at serious risk.

14.5 Requests for information by the police will be considered only where such requests are in the form of a fully completed Data Protection request form. If the request is deemed appropriate by two Senior Managers, the Head of Central Services will process the request.

14.6 When a decision to release information to the police is made only the minimum necessary information to meet the identified need will be provided. Advice should be sought from the Head of Central Services in respect of all requests for information from the police.

14.7 Where the Trust has an obligation to disclose information without consent, (for example, where required by legislation or by a Court Order), such disclosures must be approved in advance by the relevant Senior Manager.

15. PRIVACY STATEMENTS

Any documentation which gathers personal and/or special categories of personal data should contain the following Privacy Statement information:

- Explain who we are
- What we will do with their data
- Who we will share it with
- Consent for marketing notice
- How long we will keep it for
- That their data will be treated securely
- How to opt out
- Where they can find a copy of the full notice

A fuller Privacy Statement will also be published on our website.

16. OBTAINING CONSENT

16.1 Consent may be obtained in a number of ways depending on the nature of the interview, and consent must be recorded on or maintained with the case records:

- face-to-face
- written
- telephone
- email.

Face-to-face/written

A pro-forma should be used.

Telephone

Verbal consent should be sought and noted on the case record.

E-mail

The initial response should seek consent.

Consent obtained for one purpose cannot automatically be applied to all uses e.g. where consent has been obtained from a client in relation to information needed for the provision of that service, separate consent would be required if, for example, direct marketing were to be undertaken.

Preliminary verbal consent should be sought at point of initial contact as personal and/or special categories of personal data will need to be recorded either in an email or on a computerised record

(e.g. database). The verbal consent is to be recorded in the appropriate fields on the computer record or stated in the email for future reference. Although written consent is the optimum, verbal consent is the minimum requirement.

16.2 Specific consent for use of any photographs and/or videos taken should be obtained in writing. Such media could be used for, but not limited to, care planning, publicity material, press releases, social media, and website. Consent should also indicate whether agreement has been given to their name being published in any associated publicity. If the subject is less than 18 years of age then parental/guardian consent should be sought.

16.3 Individuals have a right to withdraw consent at any time. If this affects the provision of a service(s) by SJMT then the staff member should discuss with a Manager at the earliest opportunity.

17. INFORMATION SHARING

17.1 Where the Trust shares information with other organisations (for example for the provision of care or for safeguarding purposes) the relevant Manager should maintain a record of those organisations and the nature of the information shared. Where appropriate, an Information Sharing Agreement should be drawn up to cover the type of information to be shared, the circumstances and frequency under which information is shared, and any safeguards surrounding transfers of information.

17.2 Information will not be shared for purposes beyond direct care where an individual has exercised the right to opt out of sharing information for this purpose, unless there is a mandatory legal requirement or an over-riding public interest in sharing that information.

17.3 At this time, we do not share any data for planning or research purposes for which the **national data opt-out** would apply. We review this on an annual basis and for any new processing.

18. THE RIGHT TO BE FORGOTTEN

18.1 The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a. the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b. the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;

c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing;

d. the personal data has been unlawfully processed;

18.2 Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers

which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

18.3 Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

a. for exercising the right of freedom of expression and information;
b. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c. for reasons of public interest in the area of public health;
d. for the establishment, exercise or defence of legal claims.

The right to be forgotten does not apply to health and social care records.

19. ACCESS TO IT SYSTEMS

19.1 Access to systems that hold sensitive or other confidential information relating to clients or staff must be strictly controlled. The Trust IT Security Policy provides detailed guidance on implementing access control to IT systems.

19.2 Key standards are:

- Restrict access to a level appropriate to the user's role.
- Access should only be gained by means of a restricted login and, where necessary, a security password or pin number, which is issued when the appropriate training has been received and the relevant level of access has been authorised.
- Passwords must be kept secure and never shared with other users. Password sharing is treated seriously and may lead to disciplinary action.
- Users must exit to the appropriate sign-on screen when the computer is not in use.
- No computers should be placed in such a position that unauthorised persons can view client or other confidential information. If this proves to be impossible, the purchase of a privacy filter should be considered.

19.3 In some circumstances generic logins to PCs (i.e. the Windows desktop) are allowed (for example shared PCs) but access to applications that contain personal data must only be made using individual username/password.

19.4 Personal data relating to service users, their families and carers must be processed only on devices issued by the Trust.

20. INAPPROPRIATE ACCESS TO RECORDS

20.1 Access to data for which the member of staff does not have authorisation, at the time the record is accessed, is prohibited. This includes access to his/her own information without a formal request

20.2 Any staff accessing or attempting to access records they are not authorised to see may be subject to disciplinary procedures. Unauthorised access to or disclosure of information may also render the individual responsible liable to prosecution.

21. STORAGE AND DISPOSAL OF INFORMATION

21.1 All printed material containing personal data or confidential organisational information must be treated as confidential and kept secure at all times. Personal data stored electronically must be

stored only on devices that have adequate security measures in place. (See Trust IT Security Policy).

21.2 All data (manual and electronic) should be periodically reviewed to ensure that the information is accurate, up to date and complete.

21.3 No data (manual and electronic) should be kept for longer than is necessary. Data will be retained in accordance with the retention periods set out in the Record Keeping, retention and Disposal Policy.

21.4 All printed material containing personal data or confidential organisational information must be disposed of securely using the confidential waste disposal service provided by the Trust. The disposal of computer equipment and devices capable of storing information should be carried out through the Finance department to ensure all data is removed before disposal.

22. Direct Marketing

22.1 Direct Marketing is a communication that seeks to elicit a measurable fundraising response (such as a donation, a visit to a website, sign up to Gift Aid, etc.). The communication may be in any of a variety of formats including mail, telemarketing and email. The responses should be recorded to inform the next communication. Sir Josiah Mason Trust will not share or sell its database(s) with outside organisations.

22.2 Sir Josiah Mason Trust holds information on our staff, volunteers, clients and other supporters, to whom we will from time to time send copies of our newsletters, magazine and details of other activities that may be of interest to them. Specific consent to contact will be sought from our staff, clients and other supporters, including which formats they prefer (eg mail, email, phone etc) before making any communications.

22.3 We recognise that clients, staff, volunteers and supporters for whom we hold records have the right to unsubscribe from our mailing lists. This wish will be recorded on their records and will be excluded from future contacts.

22.4 The following statement is to be included on any forms used to obtain personal data:

We promise never to share or sell your information to other organisations or businesses and you can opt out of our communications at any time by telephoning 0121 245 1002, writing to Sir Josiah Mason Trust, Mason Court, Hillborough Road, Solihull, B27 2PF or by sending an email to enquiries@sjmt.org.uk

23. REPORTING BREACHES OF CONFIDENTIALITY

23.1 All information governance incidents, including actual and suspected breaches of confidentiality, must be recorded on the Report a Personal Data Breach Form. This will be monitored by the Trust's Information Governance Group which meets bi-monthly.

23.2 The Head of Central Services will review each report and if necessary request an investigation by the appropriate department/manager. This may include a Senior Manager commissioning an audit of the records accessed by a staff member on one or more electronic record systems. Where appropriate, an investigation may be deemed to warrant disciplinary action. This will be the responsibility of the line manager or the Human Resources Department.

23.3 Where a breach occurs which presents a risk to the confidentiality of a person's data, the data subject will be informed of that breach without undue delay. Where appropriate, breaches will be reported externally (for example to the Information Commissioner), using the relevant reporting mechanism.

24. COMPLAINTS ABOUT CONFIDENTIALTY.

24.1 The Trust will deal with complaints about its confidentiality processes within the spirit of the Trust's Complaints Policy and Procedure. However, complainants also have the right to complain to the Information Commissioner, but usually this is only when the local complaints process has been exhausted. For more information please refer to the Information Commissioners website.

25. TAKING PERSONAL DATA RECORDS OFF-SITE

25.1 Before any hardcopy record is taken offsite an assessment must be made as to whether the information needs to be taken offsite at all.

25.2 The removal from site of any record, especially those of a sensitive or personal nature, must be kept to an absolute minimum and should not be removed unnecessarily.

The following precautions must be taken when going on an Offsite Visit:

- All records taken offsite must be transported in a secure lockable bag/plastic wallet and never loose leaf as this increases the risk of loss or theft;
- Secure plastic wallets are available from Central Services on request;
- The secured documents must remain at all times in the possession of the member of staff transporting them and not be left unattended at any time;
- Records must not be left in a vehicle whilst it is unoccupied;
- Records must, whenever possible, be returned to base at the end of the working day. Any instance where records are not to be returned to the office on the same working day must be agreed in advance with the Team Manager or Senior Manager responsible for the relevant record/s;
- Records must be returned as soon as is practically possible;
- The responsible staff member should ensure when the documents have been returned to Trust premises, they have been filed appropriately;
- The Data Controller should be immediately informed of any data protection breaches or potential breaches – staff should follow the Data Protection & Confidentiality Policy.

25.3 Records should not normally be away from base for more than one working day. If for some reason the records can't be returned, then Data Controller must make appropriate arrangements for the records to be retrieved.

26. BREACH OF THIS POLICY

26.1 Failure to manage personal data securely places the Trust at risk of breaching data protection legislation and Trust policy. All Trust staff have responsibility for the security and proper management of the personal data and other confidential information they process.

26.2 Failure to comply with the terms of this and associated policies may lead to disciplinary action and / or legal proceedings against the individuals concerned.

APPENDIX 1 – Staff employment contract clauses

The staff contract and Employee Handbook includes a statement of confidentiality as follows:

Confidentiality

Your employment with us places you in a position of trust and confidence. During your employment you will inevitably see and use sensitive confidential information and data about people's relationship with this organisation. This may relate to other employees, clients, suppliers etc. It is important to recognise that you are dealing with privileged information.

You must not, except in the proper performance of your job or as required by law, disclose confidential information relating to our organisation. This also applies where we must respect an obligation of confidence to anyone else. This is both a legal and contractual obligation. You must respect it even after you leave our employment. Confidential information/data includes but is not limited to:-

- Sensitive information/data about other employees and those who undertake work or other activity on our behalf.
- Sensitive information/data about or received from customers, clients, suppliers etc.
- Unpublished financial accounts or statistical data.
- Trading or operational procedures, methodology or analyses.
- Processes, designs and products in development or subject to modification.

These provisions apply where you acquire the information/data through your employment with us. And where it would not be publicly available other than by your disclosure.

You must not disclose, publish or misuse such information/data. You must not supply it to any unauthorised person or organisation. This applies irrespective of whether you are doing so for your own purpose or benefit or for any other reason.

We expect you to take all appropriate action to maintain the security and sensitivity of confidential material. We also expect you to use your best efforts to prevent disclosure, publication or misuse of confidential material by others. Please report any suspected breach to us immediately.

You must not remove or transmit any of our documents, material or data physically or electronically. You must not send/store our information/data onto your own or any external storage device or medium. We must specifically authorise any deviation from this policy in advance. The only exceptions are where you do so in the proper performance of your job or as required by law.

You must return to us when we request, and in any event when your employment ends, all our documents and equipment. This includes information belonging to us which you may have stored on portable or external electronic media locations. Where we request, you must delete, destroy, remove or erase confidential information contained in documents, electronic storage media/devices, disks etc. This applies to all material in your possession or under your control, irrespective of its location.

Third Party Personal Information

Please pay particular attention to the risks of providing or transmitting confidential or sensitive information inappropriately. This is particularly important with electronic transmissions, which are notoriously insecure. Although widely used within business and public life, email may be inappropriate in certain circumstances. You must observe our internet, email and social networking policies and procedures in respect of such transmissions.

You must also be particularly careful in respect of your use of social networking sites. Making inappropriate remarks on such sites is a serious breach of our rules. This applies to all social networking sites e.g. Facebook, Twitter, LinkedIn etc. It applies to comments you make, for instance, about this organisation, other employees or those who utilise our services. It does not matter whether you are at work or you make the contribution in your own time. We regard any such breach as a potential act of gross misconduct.

You must not access the records of other employees, those who use our services, suppliers etc. unnecessarily or without authority. If you do, this will be treated as gross misconduct and it is also potentially a criminal offence.

This summarises important elements of the way in which we deal with data protection issues. However, it cannot be exhaustive. Please ensure you are clear about data protection, information you are allowed to gather, disclose, dispose of or retain. Consult a manager at the earliest opportunity if you are in any way unsure.