GENERAL DATA PROTECTION PRIVACY NOTICE, ACCESS TO FILES AND INFORMATION POLICY

Overview

A. The Company takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

B. This policy applies to current and former employees, workers, volunteers, apprentices and consultants. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

C. The Company also has policies in place relevant to job applicants, customers, suppliers and other categories of data subject in this policy and also separate privacy notices that are given to data subjects.

D. The Company has measures in place to protect the security of your data in accordance with our Data Security Policy, which is also contained within this policy.

E. The company will hold data in accordance with our Data Retention Policy. Found later in this part of the handbook. We will only hold data for as long as necessary for the purposes for which we collected it.

F. The Company is a 'data controller' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

G. This policy explains how the Company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company.

H. This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the Company at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and the GDPR.

I. This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

J. This policy should be read in conjunction with the following documents:

a) Guidance from the Information Commissioner

b) Guidance from the Care Quality Commission

c) The Code for Nurses and Midwives effective from March 2015

d) Care Act 2014 Statutory Guidance

e) Guidelines for Records and Record Keeping – NMC 31 March 2015

f) Access to Health Records Act 1990

g) Computer Misuse Act 1990

h) Data Protection Act 1998 and 2018

i) NHS Code of Practice about Confidentiality – 2003 Gov.co.uk

j) DBS Code of Practice November 2015

In this policy the following terms have the below meanings:

- **'PERSONAL DATA'** means**:**
    - information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.
    - This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.
- **'SPECIAL CATEGORIES OF PERSONAL DATA'** are types of personal data consisting of information about:
    - your racial or ethnic origin;
    - your political opinions;
    - your religious or philosophical beliefs;
    - your trade union membership;
    - your genetic or biometric data;
    - your health;

- your sex life and sexual orientation; and
- any criminal convictions and offences.

- We may hold and use any of these special categories of your personal data in accordance with the law.

1 Data Protection Principles

1.1 Personal data must be processed in accordance with six 'Data Protection Principles. It must:

1.1.1 be processed fairly, lawfully and transparently;

1.1.2 be collected and processed only for specified, explicit and legitimate purposes;

1.1.3 be adequate, relevant and limited to what is necessary for the purposes for which it is processed;

1.1.4 be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;

1.1.5 not be kept for longer than is necessary for the purposes for which it is processed; and

1.1.6 be processed securely.

1.2 We are accountable for these principles and must be able to show that we are compliant.

2 The data we hold about you

2.1 We will collect and use the following types of personal data about you:

2.1.1 recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments as well as the answers to your interview questions and results of any application process, test or assessment. We may also store or process your previous employment history;

2.1.2 your contact details, name address, telephone number, email and date of birth;

2.1.3 the contact details for your emergency contacts;

2.1.4 your gender or details of any gender reassignment;

2.1.5 your marital status and family details;

2.1.6 information about your contract of employment (or services) including start and end dates of employment/engagement, role, duties and location, working hours, details of promotion or demotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement, expense payments and wage amendment information;

2.1.7 your bank details and information in relation to your tax status including your national insurance number;

2.1.8 your identification documents including passport, photographic identification, driving licence, proof of address both past and present, your National Insurance Number and information about your immigration status and right to work for us;

2.1.9 information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings),consultation meetings about redundancy, capability, welfare, health and safety, retirement, appraising performance, informal meetings, supervision meetings, training and development;

2.1.10 information relating to your performance and behaviour at work;

2.1.11 training records;

2.1.12 electronic information in relation to your use of IT systems/swipe cards/telephone systems, clocking in and out numbers and codes, employee numbers or other employee, contractor or worker identification;

2.1.13 your images (whether captured on CCTV, by photograph or video);

2.1.14 Your voice through recorded telephone conversations or meetings;

2.1.15 any other category of personal data which we may notify you of from time to time.

3 What is processing?

3.1 **"Processing"** means any operation which is performed on personal data such as:

3.1.1 collection, recording, organisation, structuring or storage;

3.1.2 adaption or alteration;

3.1.3 retrieval, consultation or use;

3.1.4 disclosure by transmission, dissemination or otherwise making available;

3.1.5 alignment or combination; and

3.1.6 restriction, destruction or erasure.

3.2 This includes processing personal data which forms part of a filing system and any automated processing.

4 How will we process your personal data?

4.1 The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

4.2 We will use your personal data for:

4.2.1 performing the contract of employment (or services) between us;

4.2.2 complying with any legal obligation; or

4.2.3 if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights below.

4.3 We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

4.4 If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from. This in turn may then lead to the termination of your contract with us if we are not able to fulfil crucial parts of it.

5 Examples of when we might process your personal data

5.1 We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

5.2 For example (and see section 7.6 below for the meaning of the asterisks):

5.2.1 to decide whether to employ (or engage) you;

5.2.2 to decide how much to pay you, and the other terms of your contract with us;

5.2.3 to check you have the legal right to work for us;

5.2.4 to carry out the contract between us including where relevant, its termination;

5.2.5 training you and reviewing your performance*;

5.2.6 to decide whether to promote you;

5.2.7 to decide whether and how to manage your performance, absence or conduct*;

5.2.8 to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;

5.2.9 to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;

5.2.10 to monitor diversity and equal opportunities*;

5.2.11 to monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others;

5.2.12 to monitor and protect the health and safety of you, our other staff, customers and third parties*;

5.2.13 to pay you and provide pension and other benefits in accordance with the contract between us*;

5.2.14 paying tax and national insurance;

5.2.15 to provide a reference upon request from another employer;

5.2.16 to pay trade union subscriptions if relevant*;

5.2.17 monitoring compliance by you, us and others with our policies and our contractual obligations*;

5.2.18 to comply with employment law, immigration law, health and safety law, tax law and any other laws which affect us*;

5.2.19 to answer questions from insurers in respect of any insurance policies which relate to you or others*;

5.2.20 running our business and planning for the future;

5.2.21 the prevention and detection of fraud or other criminal offences;

5.2.22 to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*;

5.2.23 to comply with obligations to our local authority partners and any Regulators and

5.2.24 for any other reason which we may notify you of from time to time.

5.3 We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting your unit manager in writing.

5.4 We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

5.4.1 where it is necessary for carrying out rights and obligations under employment law;

5.4.2 where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;

5.4.3 where you have made the data public;

5.4.4 where processing is necessary for the establishment, exercise or defence of legal claims;

5.4.5 where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity; and

5.4.6 Where processing of your criminal convictions, cautions or other relevant information held by the DBS is necessary to comply with obligations under the Care Act or any other obligations imposed because we care for vulnerable adults.

5.5 We might process special categories of your personal data for the purposes in paragraph 5.2 above which have an asterisk beside them. In particular, we will use information in relation to:

5.5.1 your race, ethnic origin, religion or beliefs, age, sexual orientation or gender to monitor equal opportunities;

5.5.2 your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and

5.5.3 your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

5.6 We do not take automated decisions about you using your personal data or use profiling in relation to you.

6 Sharing your personal data

6.1 Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

6.2 We require those companies or organisations to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

6.3 We may also need to share your personal data with local authorities including safeguarding, the DBS and regulators such as the Equalities Commission, CQC and the ICO.

6.4 The legitimate activities that third parties may do for us are:

6.4.1 Providing a payroll service including providing benefits and pension schemes;

6.4.2 Providing advice to us about legal issues, the care we provide and how we run our business or accounts;

6.4.3 Providing health and safety advice and guidance;

6.4.4 Providing tax advice;

6.4.5 Providing medical opinions about you and your ability to work;

6.4.6 Providing the internet, telephone system, broadband, email, computer system and all other information or communication technology services to us.

6.5 We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

7 How should you process personal data for the Company?

7.1 Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's rules about data security and data retention.

7.2 The Company's Director of Operations is responsible for reviewing this policy and updating the Board of Directors on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

7.3 You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

7.4 You should not share personal data informally.

7.5 You should keep personal data secure and not share it with unauthorised people.

7.6 You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

7.7 You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

7.8 You should use strong passwords and comply with the Company's rules about passwords contained in the staff handbook.

7.9 You should lock your computer screens when not at your desk.

7.10 Personal data should be encrypted before being transferred electronically to authorised external contacts. Speak to IT for more information on how to do this.

7.11 Consider anonymising data or using separate keys/codes so that the data subject cannot be identified where sensible, appropriate and necessary to do so.

7.12 Do not save personal data to your own personal computers or other devices.

7.13 Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of Jane Heslop.

7.14 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

7.15 You should not take personal data away from Company's premises without authorisation from your line manager or the Operations Team.

7.16 No electronic devices such as company computers or phones/smartphones should be stored in a vehicle overnight.

7.17 Personal data should be shredded and disposed of securely when you have finished with it.

7.18 You should ask for help from Operations if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

7.19 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

7.20 It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

7.21 No personal data of any of our clients that is contained within any document should be stored outside of your place of work. This would also amount to gross misconduct and could result in your dismissal.

7.22 No unauthorised copies of any personal data of anyone should be made. This would also amount to gross misconduct and could result in your dismissal.

7.23 No photographs are to be taken by you during work time, in any place of work or extended place of work (such as on social events with work colleagues) or where any personal data about any client is captured by the photograph without the express permission of the data subject and the operations team in any situation involving clients or during working time or in the case of any extension of the work place outside of working time without the express permission of the data subject.

8 How to deal with data breaches

8.1 We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach.

8.2 If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours. Examples of serious breaches are in the ICO guidance available at your unit. If you are aware of a data breach you must contact your unit manager or the Operations Team immediately and keep any evidence you have in relation to the breach.

8.3 All breaches must be recorded in the breach register for your unit.

8.4 If you discover a breach you must therefore do as follows:

8.4.1 Make a note of the date, time, type of breach and who was involved;

8.4.2 Inform the shift leader and notify ops if it is a serious breach;

8.4.3 Complete the breach register with the shift leader and both signing it once complete;

9 Compliance

9.1 The Data Protection Commissioner maintains a public register of data controllers. Each register entry includes the name and address of the data controller and a general description of the processing of personal data. Individuals can consult the register to find out what processing is being carried out. Our registration number is PZ 537702.

9.2 The Home's Data Protection compliance officer is Jane Heslop who has overall responsibility for adherence to this policy. Any queries in relation to data protection should be addressed to the compliance officer in the first instance.

9.3 Regular reviews will be made by the Home to ensure that this policy is being complied with and Service Managers who maintain employee records must also comply with this policy. All staff should also try to keep their own and the information of others confidential. It is the duty of both the Home and the individual employee to make sure that the information maintained on the employee is accurate.

10 Client's Records

10.1 Clients in our care should be told that information on their support plans may be seen by other people or agencies involved in their care.

10.2 Clients have a right to ask to see their own support plan. Those wishing to gain access to their records should be directed to the manager of the unit in which they reside.

10.3 Clients have the right to ask for their information to be withheld from us or other health professionals. We must respect that right unless withholding such information would cause serious harm to that client or to others, or that client lacks capacity and it is not in their best interests to withhold the information. In the latter circumstances, a DOLS will be in place to confirm the authority to make that decision on the client's behalf. Organisations that employ professional staff who make records are the legal owners of those records. However, this does not mean that anyone within the organisation has an automatic right of access to the records or the information contained within them.

10.4 If there are any problems relating to accessing a record and the staff member is unable to resolve this, for instance missing records, then this should be reported to the Home Manager and recorded in the client's support plan that this has been done.

10.5 The records of any client should not be accessed to find out personal information that is not relevant to their care and support or to your duties and responsibilities as an employee.

10.6 Client's records may be used for research, teaching purposes and clinical supervision only with the express consent of the client and the operations team. The same principles of access and confidentiality remain the same and the right of the client to refuse access to their records must be respected.

10.7 Disclosure

10.7.1 Information that can identify a client must not be used or disclosed for purposes other than their care and support without the clients' explicit consent.

10.7.2 However such information can be released if the law requires it or where there is a wider public interest. Staff have a duty to protect the confidentiality of the client.

10.7.3 Under common law, information can be disclosed if it will help to prevent, detect, investigate or punish serious crime or if it will prevent, abuse or serious harm to others.

11 Subject access requests

11.1 Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to your unit manager who will coordinate a response.

11.2 If you would like to make a SAR in relation to your own personal data you should make this in writing to Krishana Devi. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

11.3 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

12 Your data subject rights

12.1 You have the right to information about what personal data we process, how and on what basis as set out in this policy.

12.2 You have the right to access your own personal data by way of a subject access request (see above).

12.3 You can correct any inaccuracies in your personal data. To do you should contact Krishana Devi.

12.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact Krishana Devi.

12.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact Krishana Devi.

12.6 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

12.7 You have the right to object if we process your personal data for the purposes of direct marketing.

12.8 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

12.9 With some exceptions, you have the right not to be subjected to automated decision-making.

12.10 You have the right to be notified of a data security breach concerning your personal data.

12.11 In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact Krishana Devi.

12.12 You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

13 Fraud Prevention and Detection

13.1 Payroll information and other information may be used by the Home in order to prevent or detect fraud.

13.2 Such information will not be disclosed to other organisations, for example the Department of Society Security, for the prevention or detection of fraud unless:

13.2.1 The employee has given their consent; or

13.2.2 The Home is required by law to make the disclosure; or

13.2.3 In the circumstances of a particular request from an organisation the Home is satisfied that if it failed to disclose the data, the prevention or detection of crime is likely to be prejudiced.

14 References

14.1 There is no obligation under the Data Protection laws for the Home to provide employees or former employees access to a confidential reference provided by the Company.

14.2 If the Home is the recipient of a reference the potential employee concerned is entitled to request access to the reference, however, the Company is entitled to take steps to protect the identity of third parties such as the author of the reference.

15 External Disclosure Requests

15.1 The Company may be requested by a third party to supply information about an employee. The Company is cautious in its response to such requests.

15.2 If an employee receives a request for information about employees, clients or anyone else, a disclosure of the information sought or any other information must not be made. The request should be referred directly to the Service Manager immediately. This is the policy for all external requests even if they purport to be from a Government body, for example, the Inland Revenue. Those seeking information may be using deception to gain access to information to which they are not entitled.

15.3 Only unit managers or above have the authority to respond to an external request for information. Employees who have authority to respond to external requests for information must establish the identity of the person making a request for disclosure before responding. Where practicable the request should be obtained in writing. Particular care should be taken with telephone requests, for example, by calling back to a known number.

15.4 Where those requesting information maintain the employer is under a legal duty to respond, ensure the request is received in writing detailing the basis on which it is asserted there is a legal duty. The employee dealing with the request should then check that this assertion is valid.

15.5 Where there is no duty on the Company to disclose, the Company may still respond to a request for information if it is satisfied that in all the circumstances it is lawful to do so.

15.6 If, to the Company's knowledge the security or confidentiality of an employee's records have been significantly prejudiced because they have been disclosed knowingly or recklessly without the Company's consent and there is a reasonable prospect of obtaining evidence as to who was responsible the matter will be reported to the Information Commissioner.

16 Communications

16.1 Employees should refer to the Home's Communications Policy.

17 Dismissal

17.1 When employment is terminated the Company will record the basis of the termination and ensure that this is accurately recorded.

18 Retention of Records on Current and Former Employees

18.1 The Company will retain certain categories of information on both current and former employees in accordance with set retention periods.

18.2 The records will be assessed on a yearly basis to ensure records are not kept beyond the set periods. Records may be kept beyond the set periods where this is justified for legitimate business reasons.

18.3 Records will be retained as follows in line with our legal and insurance obligations:

Wages/Salary/PAYE/Sickness/ Sick pay	6 years after employment ceases
Maternity/Paternity/Shared Parental/Adoption Leave/ Pay	3 years after the end of the tax year
National Minimum Wage/Living Wage	3 years after the end of the tax year to which they relate
Application Forms & Interview Notes for Unsuccessful Candidates	1 year from date of application
Staff employment- Personnel Files/Training Records/DBS/Disciplinary Records/Redundancy	6 years after employment ceases
Pensions-Pension Scheme Records	6 years 4 years for opt-out records
Duty Rosters	4 years

Risk Assessments	Retain the last until a new one replaces it.
Learning Difficulties (records of clients)	20 years after last entry or 8 years after clients death
Records/documents related to any form of litigation (complaints including accident/incident reporting)	10 years
Government Departments & Agencies -Contracts	6 years after the end of the contract
General operating policies and procedures	Retain the current version and previous version for 3 years
Incidents, events or occurrences that require notification to CQC	3 years
Use of restraint or the deprivation of liberty	3 years
Detention	3 years
Maintenance of the premises	3 years
Maintenance of equipment	3 years
Electrical testing	3 years
Fire safety	3 years
Water safety	3 years
Medical gas safety, storage & transport	3 years
Money or valuables deposited for safekeeping	3 years

Employers' Liability Insurance Certificates	60 years
Accounting documents/Tax Records	6 years from the end of the last company financial year they relate to
Health records for Hazardous Substances e.g. Chemicals	Minimum 40 years from the date of last entry
Accident forms, Records/Reports Record of any reportable injury, disease or dangerous occurrence (RIDDOR)	Minimum 3 years from the date of entry
Purchasing of medical devices and medical equipment	11 years
Clinical Audit Records	5 years
Records of destruction of individual health records (case notes) and other health related records	Permanently
External quality control records	2 years
Internal quality control records	10 years

19 Information Technology and Computer-held Records

19.1 Confidentiality of the information held is just as important in computer-held records as in all other records, including those sent by fax. Staff are professionally accountable for making sure that whatever method of communication they use is fully secure. Protocols exist which specify which staff have access to computer-held records. If in doubt seek advice from your unit manager or operations.

19.2 Staff who have access to information systems should be aware of and know how to use the tools that are available to them. If you have any doubts, please speak to your line manager.

19.3 Passwords to access information must not be shared without express permission from operations. Similarly systems must not be left open to access when they have finished being used. All computers should be encrypted, shut down after use or locked when a person is not using their computer and out of the room. All Company mobile phones should have a passcode and fingerprint ID set up so that access cannot easily be made by anyone who doesn't use the phone

19.4 Staff are accountable for any entry made by them to a computer-held record and must ensure that any such entry is clearly identifiable.

19.5 You must never email confidential information to your own personal email account under any circumstances without the permission of operations. Even with permission all documents containing any personal or special category data must be password protected to prevent access.

19.6 A breach of these rules will be treated very seriously and may amount to gross misconduct and ultimately dismissal without notice.

20 Password security

20.1 All passwords to any websites, apps, computer programs or anything else used for work purposes are the property of the Company.

20.2 All passwords must be changed every 60 days and the new passwords communicated to Sara Clark Administration, Finance and Facilities Manager immediately upon the point of being changed. Where necessary the operations team will provide you with passwords to certain systems, devices or programs.

20.3 Passwords must not include words and number combinations that are easy to guess or identify the individual's account.

20.4 All Passwords must contain at least:

20.4.1 A capital letter;

20.4.2 A number; and

20.4.3 Be at least 8 characters in length.

20.4.4 Contain no personal data such as important dates, names of any living individual, pet names or similar.

20.4.5 Example prohibited password: benji1

20.4.6 Example compliant password: Bzet0231!

20.5 One useful way to produce a password that is compliant is to pick the first letter from each word of a phrase or lyric. For example "*Richard of York Gave Battle in Vein"* would be Roygbiv followed by a number e.g. 0654 to give the compliant password Roygbiv0654. This will also allow you to remember the password easily.

20.6 Obviously the above example is now not a safe one to use and should not be used.

21 Examples of unlawful use of data

21.1 The following non-exhaustive list of policy breaches will be treated as gross misconduct unless prior express permission is sought from operations before the information is disclosed or processed:

21.1.1 Processing any personal data belonging to another or containing information about another person such as their name for purely personal use e.g. to seek from a lawyer or union representative or to support any internal disciplinary or grievance procedure;

21.1.2 Copying or retaining any client related materials such as support plans, records of care or health or medical information;

21.1.3 Copying any company documents about its business plans, financial information or clients;

21.1.4 Taking a photograph or any recording of a client with the express written consent of the client and the unit manager;

21.1.5 Taking any staff personal files away from its usual location or home with you without express consent from Operations;

21.1.6 Giving out any personal information to an unidentified individual without consent or giving information to an identified individual who is not entitled to that information;

21.1.7 Copying or retaining allocation sheets, annual leave requests/diaries/logs, logs of clocking in and out or any other documents about the working time of any other person.

21.1.8 Copying or retaining any letters or other handwritten documents about or relating to a client from any of the client's carers, medical professionals, family, friends or advisors.

21.1.9 Forwarding work emails to your personal email address.

22 Data Security Policy

22.1 We will use appropriate technical measures and organise the way the business operates to keep personal data secure and to protect everyone from unauthorised and unlawful processing. We will also use these technical and organisational measures to protect data against accidental loss, destruction or damage.

22.2 Some of the technical measures that the Company has taken are as follows:

22.2.1 All computers have been encrypted and have password protection in place;

22.2.2 The Company will install encrypted routers that will encrypt all connections from any of our homes that use our internet services;

22.2.3 All smart phones will have pass codes and finger print ID to ensure protection if stolen;

22.2.4 All smart phones use iOS which has built in encryption;

22.2.5 When devices cease to function, all hard drives and memory cards will be wiped where possible and destroyed where possible after any personal data has been safeguarded for retention purposes and in compliance with the law;

22.2.6 All computers have virus scanning software that regularly scans devices for hack attempts or stealth malicious software;

22.2.7 IT administration is conducted by an independent company to limit unauthorised attempts to reconfigure systems;

22.2.8 All server information is backed up to the cloud centrally which is also encrypted;

22.2.9 Access auditing software will be sourced and installed to check for any unauthorised access;

22.2.10 Website monitoring software will be installed so that risky website visits can be monitored to lessen the risk of malicious software and viruses being downloaded;

22.3 Some of the organisational measures that we are taking are as follows:

22.3.1 Clear policies and procedures containing the rules about data collection, access storage and use are in place including the consequences of breaching the rules;

22.3.2 All personal data in hard copy will be stored in lockable drawers and cabinets where practicable and must be kept locked when not in use;

22.3.3 Meetings with third parties will take place in designated meeting offices where no personal data will be allowed to be on display;

22.3.4 All personal files will need to be signed out and back in again if they are taken offsite and will only be allowed to be taken off site in exceptional circumstances;

22.3.5 Annually, all staff will be asked to provide an up to date record of their contact details for central support so that these can be kept accurate and up to date;

22.3.6 Mock ICO inspections will be conducted periodically to ensure compliance, identify areas where improvements are needed and drive improvements via action plans;

22.3.7 Visitors' badges and passes will be introduced so that visitors can be clearly identified when attending any of our premises.

22.4 Maintaining data security means:

22.4.1 Only people who are authorised to use the information can access it;

22.4.2 Where possible, personal data is pseudonymised, encrypted or coded to maintain confidentiality;

22.4.3 Information is up to date, relevant, accurate and suitable for the purpose it is needed for;

22.4.4 The appropriate tools, systems and organisational methods are in place to prevent, identify and halt any unauthorised processing of any personal data.

22.5 All of our contractors will be asked to certify and prove that they too are data protection compliant

22.6 General security measures in place include:

22.6.1 Ensuring that computer serves are not readily accessible and stored in a secure location;

22.6.2 All external cd's, DVD's or memory sticks are virus checked first before use and any data stored on them is encrypted and/or password protected where it contains personal data;

22.6.3 Data should be regularly backed up, updated and deleted when retention periods have expired;

22.6.4 Computers are to be set to lock when idle for 5 minutes or more and all computers are to be locked by the user when they user leaves the room where the computer is present;

22.6.5 All computer systems, security and software must be approved by the Director of Operations, the HR Director or the CEO;

22.6.6 Telephone security protocols are in place to prevent calls that fish/phish for personal data. The protocol is as follows:

(a) The full name and contact details such as phone numbers and email addresses should be obtained from the person calling including where they are calling from whether it is an organisation or a personal call;

(b) If you cannot verify who the caller is, then they should be asked to email the Company with their query;

(c) Do not allow callers to bully you into providing personal data or any other confidential information. If you are concerned about the caller, explain that you will need to take their details, end the call and refer the call to a manager;

(d) If any person will not end the conversation, becomes aggressive or threatening in any way, politely inform them that you will be terminating the call, say good bye and hang up the phone.

22.7 All data must be disposed of securely. The following methods of disposal are applicable where the item contains any personal data:

22.7.1 **Paper documents:** These must be shredded;

22.7.2 **Memory sticks, CD's and DVD's:** These must be rendered permanently unreadable broken into pieces and/or if possible shredded using a specific cd shredder where available;

22.7.3 **Hard drives and memory cards:** These must first be rendered permanently unreadable using an industry standard wiping program, then broken and ideally destroyed;

22.7.4 **Smart phones:** These should be returned to full factory settings and then destroyed;

22.7.5 **SIM cards:** These should be broken and then ideally shredded where facilities allow.

22.8 Data Impact assessments will be carried out where the processing of any data may result in a high risk to privacy, rights and freedoms. This will include a risk assessment of the purpose for the processing, the risks to the individual's rights and freedoms, an assessment about proportionality of processing and a record of what steps might be able to be taken and/or will be taken to mitigate against any risks.

23 Responsibilities

23.1 All employees, workers, visitors and contractors are responsible for assisting the Company and your colleagues to keep everyone's personal data safe;

23.2 Where you have access to personal data about other people, you are not permitted to use that personal data for any purpose other than in the proper fulfilment of your duties and/or responsibilities to the Company, our clients or as otherwise permitted by law.

23.3 You must:

23.3.1 Comply with all company policies and rules about data protection;

23.3.2 Only use information for the purpose it was gathered for;

23.3.3 Comply with all data protection laws in force from time to time and presently;

23.3.4 Ensure that you take no one else's personal data home with you from work.

23.3.5 Any breach of the data protection act by an employee will be investigated and if proven could result in the termination of your employment for gross misconduct.

24 Training

24.1 The Company is committed to training all individuals about the correct ways to handle personal data and the requirements, rights and obligations found in the data protection laws.

END.