Excerpt from Staff Manual….

33. Personal Details and Data Protection

The Data Protection Act (DPA) 2018 incorporates the UK's implementation of the General Data Protection Regulation (GDPR). It goes further to include -

- The DPA 2018 has a part dealing with processing that does not fall within EU law, for example, where it is related to immigration. It applies GDPR standards, but it has been amended to adjust those that would not work in the national context.
- It also has a part that transposes the EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. The Directive complements the General Data Protection Regulation (GDPR) and Part 3 of the DPA 2018 sets out the requirements for the processing of personal data for criminal 'law enforcement purposes'.
- National security is also outside the scope of EU law. The Government has decided that it is important the intelligence services are required to comply with internationally recognised data protection standards, so there are provisions based on Council of Europe Data

In relation to the Company, everyone responsible for using personal data has to follow strict rules called 'data protection principles' regarding holding and processing of personal data for its staff, work-seekers and individual client contacts. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Personal data means data, which relates to a living individual who can be identified from the data or from the data together with other information, which is in the possession of, or is likely to come into possession of, the Company.

Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on the data. It includes organising, adapting and amending the data, retrieval, consultation and use of the data, disclosing and erasure or destruction of the data. It is difficult to envisage any activity involving data, which does not amount to processing. It applies to any processing that is carried out on computer including any type of computer however described, main frame, desktop, laptop, palm top etc.

Data should be reviewed on a regular basis to ensure that it is accurate, relevant and up to date and those people listed in the appendix shall be responsible for doing this.

Data in respect of the following is "sensitive personal data" and any information held on any of these matters MUST not be passed on to any third party without the express written consent of the individual:

- Any offence committed or alleged to be committed by them
- Proceedings in relation to any offence and any sentence passed
- Physical or mental health or condition
- Racial or ethnic origins
- Sexual life
- Political opinions
- Religious beliefs or beliefs of a similar nature
- Whether someone is a member of a trade union

All staff are responsible for notifying their Manager where information is known or believed to be old, inaccurate or out of date. In addition all employees should ensure that adequate security measures are in place. For example:

- Computer screens should not be left open by individuals who have access to personal data
- Passwords should not be disclosed
- Email should be used with care
- Personnel files and other personal data should be stored in a place in which any unauthorised attempts to access them will be noticed. They should not be removed from their usual place of storage without good reason.
- Personnel files should always be locked away when not in use and when in use should not be left unattended
- Any breaches of security should be treated as a disciplinary issue.
- Care should be taken when sending personal data in internal or external mail
- Destroying or disposing of personal data counts as processing. Therefore care should be taken in the disposal of any personal data to ensure that it is appropriate. For example, it would have been more appropriate to shred sensitive data than merely to dispose of it in the dustbin.

It should be remembered that the incorrect processing of personal data e.g. sending an individual's details to the wrong person; allowing unauthorised persons access to personal data; or sending information out for purposes for which the individual did not give their consent, may give rise to a breach of contract and/or negligence leading to a claim against the Company or the individual employee for damages from an employee, work-seeker or client contact. A failure to observe the contents of this policy will be treated as a disciplinary offence.

Under the Freedom of Information Act, data subjects, i.e. those on whom personal data is held, are entitled to obtain access to their data on request and after payment of a fee. All requests to access data by data subjects i.e. staff, members, customers or clients, suppliers, etc should be referred to one of the directors of the Company.

Any requests for access to a reference given by a third party must be referred to one of the directors of the Company and should be treated with caution even if the reference was given in relation to the individual making the request. This is because the person writing the reference also has a right to have their personal details handled in accordance with the Data Protection Act 2018, and not disclosed without their consent. Therefore, when taking up references an individual should always be asked to give their consent to the disclosure of the reference to a third party and/or the individual who is the subject of the reference if they make a subject access request. However, if they do not consent then consideration should be given as to whether the details of the individual giving the reference can be deleted so that they cannot be identified from the content of the letter. If so the reference may be disclosed in an anonymised form.

It is the responsibility of each employee to inform the Personnel Officer of any changes to their personal details or status, including: surname, address, telephone number, marital status, names and dates of birth of children and emergency contact details and bank or building society details. Such information is important, among other things, for the correct benefit cover where appropriate to be arranged and so that someone can be contacted in the event of an emergency.

Each employee must view and be invited to sign a GDPR document regarding personal data storage, any permission can be withdrawn at any time