THE WHITEHORSE PRACTICE

Reviewed on 20/03/2019	**Milaine Borthwick-Ezekiel**	Next Review 20/03/2020
	GENERAL DATA PROTECTION POLICY	

1. Policy Statement

The purpose of this policy is to confirm The Whitehorse Practice's commitment to protecting the information and personal data it holds about its own employees, and also personal data, special categories of personal data and information it holds about patients' employees, ex-employees, contractors or temporary workers and prospective employees.

By the nature of its work activities providing national health services, the Practice is regularly entrusted with personal data (including health) and information by its patients and employees, and this policy aims to show how it can and will be processed, used, stored and safeguarded. All information provided to the practice by patients is treated as highly confidential (each contractor or employee will be asked to sign the confidentiality statement in appendix 1). It will be used for normal business processing purposes only. This policy also acts as a Privacy Statement and is easily available to employees in accordance with the regulations.

GDPR provides the following rights for individuals:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

2. Scope

This policy covers the practice's standards and procedures in respect of data which relates to employees, and also personal (including health) and special categories of data which is held and processed on behalf of Patients. As personal and special categories of personal data is also held on behalf of Patients, this policy covers that too.

All employees of The Whitehorse Practice and any contractors or associates who may work with us are required to comply with the standards and rules detailed here. Umar Sabat

(IG Health) is the person responsible for complying with GDPR requirements, and is the organisation's nominated Data Protection Officer.

3. Definitions

In this policy, the following definitions generally apply unless otherwise explained:

- **Practice** is The Whitehorse Practice
- **Patients are** individuals who are registered with the practice for the purpose of health care.
- **Data Controller** is the person who "owns" and decides what should be done with personal data held by the Practice.
- **Data Protection Officer** is the person with expert knowledge of the data protection law and practices and has a detailed understanding of the organisations business, the purposes for which it processes or intends to process personal data.
- **Data Processor** is the person who processes personal data on behalf of the data controller, but who has no long term interest in such data.
- **Data Subject** is the living individual(s) about whom personal data is being collected or processed.
- **Personal Data** is data which relates to a living individual who can be identified from that data or who can be identified by reference to an identifier such as e.g. name, identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, culture or social identity of that person.
- **Prime Contacts** are the individual(s) defined in the Practice's Service Agreement with its Patients, whose instructions are followed, and who may authorise the Practice to obtain and share data with other managers or directors in their respective organisations.
- **Special Categories of Personal Data** is personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, physical or mental health conditions, criminal offences, or data concerning a person's sex life or sexual orientation.

4. Consent

4.1. Consent will be obtained from Data Subjects to have, use, process and retain data where this is deemed necessary or is specifically required under the regulations.

4.2. Explicit consent will not be sought or required from Data Subjects in order to deal with day to day employment issues relating to the Practice's employees, this will be covered by the practice's policies and procedures.

4.3. Explicit consent from each Data Subject will not be sought in order to process ordinary personal data for legitimate business transactions, i.e. supporting and dealing with issues for a client where that client has provided the necessary data to the Practice for that purpose.

4.4. Consent will not be sought from Data Subjects to share data with appropriate authorities or other organisations where there is a legal requirement to do so, and such data will be shared from time to time as appropriate.

4.5. For the purposes of recruitment on behalf of patients, a statement will be included in all cover emails to confirm the data subjects information will be shared with the associated client only.

5. Employee Data & Rights

5.1. Personal and special categories of data about Practice employees will be held and processed for the purposes of usual business administration, including processing employment status, pay and other benefits, and may be passed to providers and 3rd party suppliers for this purpose.

5.2. Employees may request sight of their data through a Data Subject Access Request at any time in accordance with prevailing legislation.

6. Categories of Data

6.1. Personal and special categories of data about Practice employees will be held and processed for the purposes of legitimate business.

6.2. Data will be held and processed by the Practice for legitimate business purposes, and to comply with legal obligations. This may therefore include a range of the following about individuals as is necessary to the work being undertaken:

- Full name,
- Home address,
- Email address,
- Home telephone number and/or mobile number,
- Pay and remuneration information,
- Date of birth,
- Nationality/citizenship and passport/visa information,
- Work performance and training history,
- CV with information about education (or information about planned college/ educational courses in the case of apprentices),
- Health information and medical certificates/information which relates to absence of workplace adaptations or medical conditions and disabilities recognised under the Equality Act,
- Social media and other on-line public presence and contact points such as Twitter or blogs,
- Family and data relating to family members, lifestyle or social circumstances where they may relate to application of workplace policies, or are relevant to specific investigations,
- Any aspect of protected and personal characteristics or behaviours which may be relevant to investigation processes such as health records, race or ethnicity, trade union membership status,
- CCTV footage of individuals may be seen and retained in electronic format as evidence as part of investigation processes.

This list is not exhaustive

7. Storage of Data

7.1. Patient data is stored electronically on EMIS (EGTON) the Practice's clinical software. For other administration purposes the software used is primarily Microsoft Office (Word/Excel/Power-point), but data can also be held in photo format (e.g. sickness certificates) and pdf. This can be accessed through 21 desktop computers which have password protection security unique to users, firewalls and anti-virus software protection systems in place. Backups are kept on external hard drives on the premises in an encrypted format, password protected. For some meetings a digital recorder is used (e.g. disciplinary and investigation) the information is transcribed and shared with the relevant parties. Once the transcript has been confirmed as a true account the recording is deleted. The recorder is kept in a locked cabinet, except when travelling to meetings, where it is retained by the practice manager.

7.2. Email is accessed through NHS Mail on the practice's computers, and can be accessed directly from the server. Fasthosts are the webmail provider and have secured services.

7.3. Access to electronic data is strictly restricted to Practice employees and associates, and for the purposes of providing technical IT support only, to the IT support provider.

7.4. Data may be transferred between computers (including between the Practice's and the CCG's computer) using email and the Practice's USB stick for practical purposes. This USB stick is clearly marked with a name, and remains in the possession of a Practice employee at all times. Information moved from one machine to another using it is deleted immediately it is no longer required for security purposes because such small items are easily mislaid.

7.5. Paper medical records containing personal data are held in locked records rooms and are only removed upon request of a clinician. Access to third parties is not allowed (except as required by law).

8. Sources of Data

8.1. Data may be obtained and collected from employees, from patients, and from job applicants who respond to advertisements or approach the Practice directly.

8.2. Patients and employee's who provide personal or special categories of data to the practice for national health services or for employment purpose have the appropriate consent recorded on the medical notes or employee file to share that data with other legitimate organisations such as HMRC Sage Payroll etc.

8.3. Data is not purchased or obtained by the practice from marketing agencies or sales houses, and is not bought for marketing or sales purposes.

9. Recipients of Data

9.1. Data will be shared with patients where it relates to their health and employees in relation to recruitment/employment. It will be shared with prime contacts as defined in the Practice's Service Agreements with its patients or with approved contacts (with consent).

9.2. The Practice will never share, sell, rent or trade any personal data or information to any third parties for marketing purposes.

10. Transfer of Data outside the EEA

11. Personal and special categories of data held by the Practice on behalf of a patient will only be transferred to countries outside the European Economic Area (EEA) on a patient/next of kin/carer or employee's direct instruction. This can happen in cases death of a family member or when a patient has emigrated to another country and requests the practice to send their medical notes. Medical notes sent/posted abroad will always be by recorded delivery or secure encrypted email.

12. Length of Time Data will be Retained

12.1. At least once a year, paper and electronic files will be reviewed, and unnecessary data erased or destroyed.

12.2. Handwritten notes are routinely made relating to patients or employee contacts, telephone conversations, meetings and work undertaken for patients or employees. These are retained as a record on patients notes or employee file and will be kept for a period of 5 years. These are retained for legal purposes as they can be called

for review as evidence in Employment Tribunals or other Court actions, the practice has a legitimate reason to retain them in order to be able to recall past events. Notes are kept in secure locked cabinets or desk top for employees or on clinical software for patients.

12.3. In the case of information and reports produced in connection with investigations, grievance and disciplinary cases, which may result in legal action or a need to provide information to patients or employees to be used in evidence for legal actions sometime after the event, data will generally be kept for a period of 5 years.

12.4. Personal data will be erased without undue delay on request where:

- it is no longer necessary for it to be retained for the purposes collected or held
- the Data Subject withdraws consent to it being held (if applicable)
- there is no overriding legitimate interest of reason for processing and the Data Subject objects
- if the data was unlawfully processed, or must be erased in order to comply with a legal obligation; or

13. Data relating to Recruitment Projects

13.1. Candidates providing applications and personal data to the Practice will be advised that their information will be stored, by means of the following statement being attached to job advertisement:

13.2. It is assumed that you give consent for any personal or special categories of personal data which you submit as part of an application for this position to be processed by The Whitehorse Practice. Any personal or special categories of data you send to the practice will be used solely for the purposes of recruitment and selection in respect of the position for which you have applied. If your application is unsuccessful , your personal data will be erased from our systems within 1 year, except to retain a log of your name in order for us to retain a record of your having been an applicant for this role. This will be retained indefinitely. We will only retain your CV, covering letter/ email and any data contained in those files if you ask us to keep it for future reference in respect of any other job opportunities which may arise. If your application is successful, all personal data including interview notes will be stored in employee files and will then be erased from our records within 1 year. You are advised of your right to make a subject data access request in accordance with the GDPR, or to raise any complaints about data handling to the ICO through www.ico.org.uk

13.3. CV's of applicants who are rejected without interview will be immediately deleted after their basic information has been logged (as explained above).

13.4. CVs and interview notes of candidates who are rejected following telephone screening by the practice will be deleted 6 months after their application was processed, but basic summary information will be retained

13.5. CVs, telephone screening and personal interview notes made by the practice of candidates who are rejected following interview by patients/Practice will be deleted 1 year after their application was processed, but basic summary information will be retained.

13.6. CVs, telephone screening notes and personal interview notes made by the practice of candidates who are offered employment will be retained in employee files. .

14. Suppliers & Sub Processors

14.1. Third party suppliers and Sub Processors who may process personal data held and provided to them by the practice, e.g. Sage the Practice's payroll provider are required to provide assurances that data is held and processed in accordance with the regulations on appropriately secure systems, and with appropriately safe and secure recordkeeping and storage facilities in place.

14.2. The Practice does not use any automated decision making software to process or evaluate data without human intervention.

14.3. The only other parties to whom personal and special categories of personal data is disclosed is HMRC and Companies House to whom it is given for legal reasons.

15. Breaches & Complaints Procedure

15.1. Any personal data breaches or situations which compromise the security of patients or personal or special categories of personal data will be reported by the practice to the DPO (Umar Sabat) and ICO within 72 hours where feasible (or without undue delay). Data Subjects will also be notified IF the breach is likely to result in a risk to their rights and freedoms

15.2. Any complaints about the retention or processing of personal data should be addressed in the first instance to the Practice Manager, and sent by email to Milaine Borthwick-Ezekiel, m.borthwick-ezekiel@nhs.net

Employees and patients have the right and are also at liberty to contact the Information Commissioner, (www.ico.org.uk) who is the official who enforces data protection legislation in the UK, should they deem it necessary and appropriate to do so.

Policy approved by:	Dr Joy Nwufoh (Senior Partner)
Date:	01/03/2019
Practice Data Protection Officer:	Umar Sabat (IG Health)
Practice Caldicott Guardian:	Dr Joy Nwufoh
Practice IG Lead:	Milaine Borthwick-Ezekiel (Practice Manager)