Netherfield House Surgery

Version:	Review date:	Edited by:	Approved by:	Comments:
1.0	31.5.19	PA	AR	

Data protection policy and protocols

1.0 Purpose and scope

1.1 The purpose of this policy is to describe how the processing of personal data is undertaken at Netherfield House Surgery. It describes our approach to meeting our obligations in respect of the processing of personal data, and ensuring that in carrying out our work we can comply with the Data Protection Act 1998.

1.2 This policy shall apply to partners and employees of the practice and any other person or organisation required to process personal data on our behalf.

2.0 Policy statement

2.1 **Netherfield House Surgery** is registered as a Data Controller with the Information Commissioners Office (ICO) under the Data Protection Act 1998 (the Act). The Act imposes conditions relating to the collection, usage and handling of personal information.

2.2 The scope of activities which forms the basis for our registration as a Data Controller is defined as Healthcare under reference number **Z5872189.**

2.3 During the course of our activities, staff will gather, store and process personal information and must recognise the need to treat it in an appropriate and lawful manner.

2.4 The types of information that we may be required to handle include details of current, past and prospective partners, employees, suppliers, business associates, patients and others with whom we communicate. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Act and other regulations. The Act imposes restrictions on how we may use that information.

2.5 This policy sets out our rules on data protection and our approach to meeting the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.6 Legislation places specific responsibilities on us, as a Data Controller, and our staff, recognising that an act of non-compliance may lead to legal prosecution. It may also damage our reputation. Data protection is a matter of good business and social responsibility. To ensure that an appropriate level of data protection is maintained, this policy must be observed in relation to the collection, holding, use and disclosure of personal information.

2.7 Regular monitoring and reviewing of the effectiveness of this policy will take place to ensure that it continues to achieve its stated objectives.

2.8 Any breach or suspected breach will be investigated and may lead to disciplinary action where that breach arises as a result of the action of a staff member. In some cases a breach of the terms of this policy may be treated as gross misconduct, leading to the summary dismissal of any employee who is found responsible.

3.0 Definition of data protection terms

3.1 "**Data"** is information that is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **"Data subjects"**, for the purpose of this policy, include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3 **"Personal data"** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

3.4 **"Data controllers"** are the people who (or organisations that) determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We registered with the UK Information Commissioner's Office (ICO) as a data controller for all personal data that we use.

3.5 **"Data users"** include staff whose work involves using personal data. Data users have a duty to protect the information they handle by complying with this data protection policy and its protocols at all times.

3.6 **"Data processors"** include any person who processes personal data on behalf of a data controller. The staff of data controllers are excluded from this definition, but it could include suppliers that handle personal data on our behalf.

3.7 **"Processing"** is any activity that involves the use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **"Sensitive personal data"** includes information about a person's physical or mental-health condition, racial or ethnic origins, political opinions, religious or similar beliefs, trade union membership, or sexual life. It also includes data about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings, or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4.0 Protocols for data protection compliance

4.1 **Paul Atkinson – Practice Manager** is the assigned person/role within **Netherfield House Surgery** with functional responsibility for co-ordinating and maintaining our data-protection registration process and who will advise on any issue in relation to compliance with this policy.

4.2 Partners and line management are responsible for ensuring that employees and suppliers/service providers understand and carry out their responsibilities under the Act and this policy.

4.3 All staff are responsible for informing **Paul Atkinson – Practice Manager** of any new processing activity, or amendments to existing processing activities, of personal data.

4.4 Hard-copy and electronic media containing personal information must be securely stored to protect them from unauthorised use, or from activity that threatens the availability, confidentiality and/or integrity of personal data.

4.5 Personal data must not be disclosed to unauthorised persons other than in accordance with this policy.

4.6 Correspondence received from members of the public and/or employees requesting information under the Data Protection Act, or making any reference to the Act in regard to our work, must immediately be forwarded to Paul Atkinson – Practice Manager.

4.7 Every staff member must understand their responsibilities for data protection.

5.0 Data protection principles

5.1 Any person processing personal data must comply with the eight enforceable principles of good practice and observe any instructions issued in relation to the processing of personal data. These principles provide that personal data must:

- be processed fairly and lawfully;
- be processed for limited purposes and in an appropriate way;
- be adequate, relevant and not excessive for the purpose;
- be accurate;
- not be kept longer than necessary for the purpose;
- be processed in line with data subjects' rights;
- be secure; and
- not be transferred to people or organisations situated in other countries without adequate protection.

5.2 <u>Fair and lawful processing</u>

i. The Data Protection Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is, who the data controller's

representative is, the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

ii. For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

5.3 Limited purpose and appropriateness

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

5.4 Adequate, relevant and non-excessive processing

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data that is not necessary for that purpose should not be collected in the first place.

5.5 Accurate data

Personal data must be accurate and kept up to date. Information that is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of personal data at the point of collection and at regular intervals thereafter. Inaccurate or out-of-date data should be destroyed.

5.6 Timely processing

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. Guidance on how long certain data is to be kept before being destroyed will be given by the Practice Manager.

5.7 Processing in line with the data subject's rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

i. request access to any data held about them by a data controller;
ii. prevent the processing of their data for direct-marketing purposes;
iii. ask to have inaccurate data amended; or,
iv. prevent processing that is likely to cause damage or distress to themselves or anyone else.

5.8 Data security

i. We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss. Also, our reputation relies on managing data protection effectively to avoid potential adverse publicity and reputation damage from any failure.

ii. The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third party's data processor if they give explicit agreement to comply with those procedures and policies, or if they put in place adequate measures themselves.

iii. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:
- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should not normally, therefore, be stored solely on our individual PCs.

iv. Security protocols include:
- **Entry controls:** Entry and movement around the premises must be strictly controlled through appropriate authorisation and unauthorised persons seen in entry-controlled areas should be reported.
- **Secure, lockable desks and cupboards:** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of disposal:** Paper documents should be shredded or securely disposed of through approved means. Digital/optical media should be physically destroyed when they are no longer required.
- **Equipment:** Data users should ensure that individual monitors do not show confidential information to passers-by and that they lock/log off from their PC when it is left unattended.

6.0 Dealing with data subjects' access requests

6.1 A formal request from a data subject for information that we hold about them must be made in writing. A fee is payable by the data subject for provision of this information.

6.2 Any staff member who receives a written request should forward it to Paul Atkinson - Practice Manger immediately.

7.0 Providing information over the telephone

7.1 Any employee dealing with telephone enquiries should be careful about disclosing any personal information held by us.

7.2 In particular the employee should:
- check the caller's identity to make sure that information is only given to a person who is entitled to it;

- suggest that the caller put their request in writing if they are not sure about the caller's identity (and if their identity cannot be checked); and/or,
- refer to their line manager for assistance in difficult situations. No-one should be bullied into disclosing personal information.