**Data Security Policy**

**Guidance Notes**

It is essential that you complete the security policy with the security procedures that are relevant to your practice while always seeking to improve where possible. Please ensure that you amend the policy as required.

This policy should be completed and read in conjunction with the Mobile Working Policy and the Data Retention and Disposal Policy.

**DATA SECURITY POLICY OF:**

**[INSERT NAME OF HEALTHCARE PROFESSIONAL]**

**[INSERT BUSINESS ADDRESS]**

**[INSERT ICO REGISTRATION NUMBER]**

**[INSERT DATE]**

**Policy became operational on: [1 January 2023]**

**Next review date: [1 January 2024]**

**Data Security Policy**

**Introduction**

In order to meet the requirements of the UK GDPR, as a self-employed healthcare professional I am obliged to have in place a framework designed to ensure the security of all personal data during collection, processing and disposal. I am committed to complying with relevant data protection legislation.

**Scope of the policy**

This policy relates to the retention and storage of all personal data held in hard copy, i.e. on paper, on physical devices like USBs, CDs, DVDs, tablets and smartphones, voice dictation devices and the retention and use of electronic data.

This policy applies to:

* All use of information and information technology on [practice address] premises and at my primary residence;
* All information technology provided by the practice wherever it is used, including by employees working away from [practice address]; and
* Any employees I may have, including temporary employees, casual employees and agency staff.

**Risk assessment**

A data security risk assessment will be carried out by me annually.

The purpose of the assessment is to establish the potential risks for unauthorised access to personal data and to define appropriate actions to eliminate, or at least mitigate, the risk of unauthorised access.

**Third parties**

Arrangements must be in place to ensure the security of all personal data which may be transferred to, or processed by, a third party.

In advance of any external transfer of personal data, I am required to consider whether such a transfer is authorised under any relevant Data Sharing Agreement or is otherwise required by or permitted under the UK General Data Protection Regulation. The purpose, fairness and transparency of any transfer must always be considered.

Where external data sharing has been considered necessary or is permitted, the appropriate security precautions should be taken to minimise the risks of loss of data and/or accidental third-party disclosure.

All communications should be marked strictly private and confidential and addressed to a named individual.

Physical devices containing personal data, e.g. USBs, CDs, DVDs, must always be encrypted before being removed from the premises.

The most appropriate secure method of sending the information must be considered, e.g. hand delivery, registered or recorded delivery, courier, encrypted or secure electronic transfers.

**Disposal of personal data**

Personal data will be retained only for the designated periods as per my Retention and Disposal Policy.

All personal data must be disposed of securely and safely in accordance with the Retention and Disposal Policy.

**Security incidents**

All incidents where the security of personal data or IT systems has been compromised, or where there have been any suspected security weaknesses or threats, must be immediately reviewed and, where appropriate, remedial action taken by me.

I, as Data Protection Lead, will decide in the particular circumstances of the breach whether it is serious enough to inform the Information Commissioner’s Office.

**Appendix 1**

**Good Practice Guidelines**

**General**

1. Always log off or lock a computer or device before leaving it. This is to ensure that no one else can access your information or has the opportunity to use your workstation without identifying themselves, e.g. to send an abusive email in your name.
2. When confidential work is being carried out, ensure no one else can read the screen, for example sitting beside you on a train.
3. Protect equipment from physical theft. This is vitally important for portable equipment.
4. All devices should be patched with the latest security-critical and up-to-date patches.
5. All data storage devices, including laptops, USB sticks, voice dictation devices, CDs and DVDs, in use must be checked for viruses on every occasion before use.
6. All workstations shall be continually running approved virus-scanning software with a current virus database.
7. Where I purchase a new device that will be used for work purposes, I will register it in the IT Device Register and where applicable with my IT provider/ manager.
8. [INSERT/ DELETE MEASURES AS APPROPRIATE].

**Keeping personal information secure**

1. All personal data, whether in hard copy or stored on a USB, CD, DVD, or other physical device, must be kept in a secure environment with controlled access. Appropriate secure environments include:

[Amend as necessary and insert relevant security measures undertaken in your practice]

* locked metal cabinets with access to keys limited to authorised personnel only
* locked drawers in a desk (or other storage area) with access to keys limited to authorised personnel only
* locked rooms accessed by key and/or coded door lock where access to keys and/or codes is limited to authorised personnel only

1. Where access to personal data is required on a frequent basis, and therefore maintaining locked drawers or cabinets at all times is impractical, steps must be taken to ensure authorised personnel are in attendance at all times when the data is in an unlocked environment.
2. Files containing personal data must never be left unattended while removed from their normal locked storage area.
3. A clear desk policy in relation to files and documents containing personal information is in force at all times.
4. When any staff members, including temporary staff members, are employed in posts which involve access to and the processing of personal data, confidentiality agreements should be included within the Terms and Conditions of Employment.
5. The occasions when personal information is photocopied or printed should be kept to a minimum. Printed documents will be retrieved from the printer immediately and will not be left unattended.
6. Where I take hard copy files containing personal data out of my secure office, appropriate security precautions must be taken to guard against theft, loss or inappropriate access.
7. All manual records will be kept in a locked case whilst in transit and never left unattended in a public place or in a car.
8. I will ensure that all reasonable precautions are taken to secure data at home such as lockable cabinets, secure locked office, burglar alarm.

**Electronic devices**

The electronic storage of personal data requires certain minimum levels of security. [Amend as necessary and insert relevant security measures undertaken in your practice].

1. All personal computers/devices used for work must be protected by up-to-date anti-virus and anti-spyware software, subjected to regular virus scans, and protected by a firewall appropriate for the computer used.
2. The operating software must be checked regularly to ensure that the latest security updates are downloaded.
3. Access to all computers must be password protected.
4. Particular care must be taken to avoid potential infection by malware, e.g. by downloading software other than from trusted sources.
5. Work-in-progress should be regularly backed up, and backup media should be locked away securely.
6. Computers used for working on personal data at home should be protected from unauthorised and unrestricted access by third parties, including family members. Where practicable, the ideal is a computer used only for work.
7. The use of removable storage media (such as memory sticks, CD-ROMs, removable hard disk drives and PDAs) is prohibited and are only to be used in particular circumstances and only encrypted removable storage media devices are permitted.
8. Laptop computers must be encrypted to such standards as may be approved by my IT provider.
9. Where I access emails from my mobile telephone or potable device, I will ensure that the device is encrypted.

I will maintain a log of all computers and devices used for storing or working on personal data. The log records the type, model and serial number of each device, together with the details and currency of any anti-virus, anti-spyware, encryption or other security software maintained on each machine. I will only use devices that are on this log.

**Email and internet use**

1. Always check the address line before sending a message and check it is being sent to the correct person. Ensure the automatic email address filler is turned off or used with extreme caution.
2. Always encrypt any attachments which contain special category data, as defined under the UK GDPR.
3. Consider using an email ‘delay’ function when sending any emails which contain special category data, as defined under the UK GDPR.
4. Delete electronic mail messages when they are no longer required, in accordance with the data retention and disposal policy.
5. Do not make comments or express views that could be regarded by others as offensive or libellous.
6. Personal private emails must be saved in a separate folder from work-related emails. Clearly mark all emails that are of a personal nature as ‘personal’.
7. Do not open email attachments received from unknown senders as these may contain viruses, email bombs, Trojan horse code or some other form of malware.
8. Do not forward electronic mail messages that have been sent to you containing personal data to other individuals or groups without the permission of the originator.
9. Do not participate in chain or pyramid messages or similar schemes.
10. Do not unnecessarily send excessively large electronic mail messages or attachments.
11. Report any unusual or suspect email messages or network activity to your IT provider.
12. [INSERT/ DELETE MEASURES AS APPROPRIATE]

**Passwords**

1. All devices must be protected with a password.
2. Passwords must be kept secure and never shared with anyone else.
3. Passwords must be [at least 7 characters long and include alpha, numeric and at least one other character]. Their structure must make them hard to guess.
4. Passwords should never be displayed on screens and/or written down for ease of remembering.
5. Passwords must be updated regularly.
6. If at any time you think someone may have discovered your password, you must immediately change it or request that it is changed.
7. [INSERT/ DELETE MEASURES AS APPROPRIATE]