# iPET Network - Data Encryption Policy

iPET Network takes it's responsibility for obtaining, using and storing data seriously. As such it wishes to ensure that all data held by the organisation electronically is adequately protected from loss and inappropriate access, whether by accident or theft. Furthermore, under the Data Protection Act 2018, iPET Network is required to have in place appropriate policies and procedures which ensure the secure storage of data covered by the Act at all times.

To reduce the risk of unauthorised access to data held by the company on electronic and mobile devices iPET Network has established a comprehensive policy of data encryption. This covers data which can be accessed from outside the organisation, and which can be removed from the organisation.

This policy covers data stored by the following means:

- Laptops and PCs
- Handheld portable devices such as mobile phones, PDAs and Tablet devices
- Portable storage devices such as USB data sticks, external drives
- Removable media such as DVDs, CDs, floppy disks etc

**Implementation**

Encryption will be applied to relevant files on all static PCs located at iPET Network premises, in order that data stored on these computers will be automatically encrypted. Users of these PCs will not be asked to supply a specific password for individual documents or files (unless there is a specific need for a document to be password protected/encrypted) once they have logged into their PC.

Access to the organisation's MIS (management information system), will require a separate user name and password. Staff are advised that this password be changed on a regular basis and that it is different from their network password

The default encryption applied above will also apply to laptops owned by iPET Network, a minimum of a 6-digit alphanumeric or numeric passcode will be used to encrypt handheld portable devices such as Tablet Devices. All devices will be managed by iPET Network and Data Protection will be enabled.

Portable storage devices such as USB data sticks will be encrypted before use with individual passwords in order that their portability is maintained. iPET Network prohibits the use of non-encrypted data storage devices at all times; and has suspended the use of USB ports to ensure compliance with the policy.

Removable media such as CDs and DVDs drives will also be read only meaning they cannot be used to remove data.

Staff have access to an iPET Network owned and managed online cloud storage account and use it as a means of moving and sharing documents. This online account should only contain documents that hold no personal data e.g. whole organisation timetables, policies and individual planning.

If a handheld device cannot be encrypted it must not be used to store person identifiable data. Furthermore, it must not be connected to any other of iPET Network systems, whether by physical (e.g. USB) or wireless connection (e.g. Wi-Fi). The organisation may run a guest SSID identified as Guest on some of its premises to ensure no device can gain direct access.

iPET Network aims to replace any devices which cannot be encrypted and which are capable of storing personal data where it is possible to do so.

**Compliance**

The encryption process will be managed by the organisation's Directors. Passwords will be kept confidential by users and will adhere to the guidelines defined in the organisation's IT Policy. Passwords will be renewed on a 90-day basis.

Users will not remove or copy sensitive or personal data from iPET Network premises unless the data storage device is encrypted and is transported securely for storage in a secure location.

Staff are reminded that Emails should be treated as public property and therefore should contain as little personal data as is possible.

Users must protect all portable and mobile devices used to store and transmit personal information using approved encryption software.

Sensitive or personal data must be securely deleted when it is no longer required.

Non-compliant devices may be detected and disabled using management systems installed for this purpose without notice.

Users' privately owned mobile computing equipment or portable devices will not be permitted to connect to the organisation's network. The one exception to this rule will be through remote desktop.

## Document Control

**Document Name: Data Encryption Policy**

**Document Number: P9**

| Date of Correction | Version Number | Correction Reason |
|---|---|---|
| | 1 | |
| 13/01/2022 | 2 | Annual policy review |
| 02/11/2023 | 3 | Annual policy review |