2.3

AISCT maintains a legitimate basis for which personal information is processed and will not process personal information if there is no legal obligation and/or legitimate interest and/or consent.

6.4. Fur

7.3. IT Di

- save copies of personal information directly to their own private computers, laptops, tablets or mobile devices;
- share personal information informally or by means of unencrypted electronic communications (email, text message, etc.)
- transfer personal information without the express permission of the Information Officer.

Persons are responsible for:

- taking sensible precautions to keep all personal information they come into contact with secure;
- keeping areas where personal information may be found organized and to a minimum, with all confidential information out of view from unauthorized persons at all times;
- ensuring personal information is encrypted prior to transmitting electronically (the IT Director will assist where required);
- making sure all computers, laptops, tablets, mobile devices, flash drives and any other device containing personal information is password protected and never left unattended where it may be accessed by an unauthorized person. Passwords must be changed regularly and never shared with unauthorized persons or stored as text in-text;
- switching off devices or locking the screen when not in use (external drives, CDs, DVDs and other removable storage devices must be locked away when not in use);
- undergoing and taking proper note of awareness training provided to them;
- ensuring personal information is never discussed in public areas or with unauthorized individuals

Should a person suspect or be aware of any security breach or breach of this policy, they must immediately report it to the Information Officer.