Information Security

Office Security

- Offices at Haverfordwest have security alarms fitted and door security systems in operation. These are operated in accordance with guidelines provided and tested weekly.
- On vacating rooms at the end of each day, staff are expected to ensure that all windows and doors are secured and locked and that blinds or curtains on the ground floor have been closed.
- Computer equipment must be turned off unless requested otherwise by ICT Staff.
- Procedures for dealing with visitors to the offices are to be always complied with, giving limited access to certain areas.

Hardware Protection – Workstations

- Each member of staff is responsible for ensuring that their machines are locked away safe.
- Portable equipment used outside of the Group offices are to be used in compliance with guidelines provided by the Group.
- All portable equipment is logged to staff by an ICT Officer and have mobile device management installed.(Airwatch)
- Computers should be shut down during thunderstorms to prevent damage.

Hardware Protection - Network Servers

- The network servers are in a specially constructed security cabinet in a designated secure room.
- Systems are protected from power failure and supply interference using surge protection and battery backup systems.
- In the event of power supply failure, the systems are configured to automatically shut down within the time allowed by the battery backup system.
- System hardware is to be suitable to enable one server to be used to replace the other in the event of serious system failure.
- System hardware is to be covered by a maintenance SLA contract provision.
- Network cabling has been installed and configured to provide minimal interruption to service in the event of component failure.
- An air conditioning system is used to keep equipment at its optimum temperature at all times.

Software Protection – Network

- Passwords are to be enabled for all users who wish to access the network, Passwords are set to never expire and required to be a minimum of eight and a maximum of twelve characters and must include a combination of letters, numbers and special characters.
- Network configuration is to be restricted for all users except for designated administrators.
- The network administrator shall restrict access to areas and directories to prevent files from being read, saved, or amended by users who do not normally require such access rights.
- Administration passwords are to be changed on a regular basis and not disclosed to anyone.

Software Protection – General

- Where the facility to operate password protection of software exists, it should be enabled.
- Installation disks should be backed up and one copy stored away from the office offsite.
- All software used by the Group must be licensed according to the manufacturer's rules.
- No software shall be installed onto the Group`s equipment without the authorisation of the ICT Staff.

Data Backup

- Data backups are made daily for Outlook emails/MS Teams & One Drive.
- All data is held on a storage unit in a secure environment only accessible to authorised ICT staff.
- One copy of the data is also always stored away from the office offsite in a secure location.
- The use of portable disk/drive for means of storing and transporting data is not allowed.

Virus Protection

- All servers and workstations are to have anti-virus software installed and enabled.
- Staff who have laptop computers are to ensure that their machines are made available to the IT Officer upon request for virus updates to be installed.
- E-mails are to be checked before reaching our mail server by diversion to a 3rd party virus checking system.
- Anti-virus software is enabled to check files on drives as a matter of routine.
- Where there is any doubt regarding the possibility of a disk supplied to the Group having a virus, the disk should be passed to ICT Staff for checking before it is used.
- Virus software shall be configured so that all reports are made to the system administrator as well as the user. However, there is still an obligation upon staff to inform ICT Staff immediately of any problems.
- Periodic testing of virus defences/reports are undertaken by ICT Staff.
- The Baracuda Phishline Campaign tool to be carried out on a quarterly basis to assess if there are further training requirements for staff, this will be carried out

by ICT

Firewall

- All External Network traffic must pass through a firewall system for internet and telecoms.
- All security patch/updates are done by a third-party support supplier as per the terms in the SLA agreement.
- Any security requirements are routed through a DMZ route to give additional security.
- A system log will be held and accessed to monitor internet sites accessed, time used and to limit access to inappropriate material/sites.

Software Protection - Service Providers

- Some service providers have their own security systems for their software and the security systems provided are to be always used.
- Passwords must not be disclosed to anyone else or left written down.

Remote Access

- Users accessing the remote systems data are defined as remote users and will be required to take all precautions to ensure all passwords or unauthorised access to the Group's systems are not compromised.
- Special security measures must be in place to ensure that only authorised users are able to access the system. Measures adopted should include additional password protection and caller recognition to authenticate permitted users and data encryption to prevent unauthorised interception.

Third Party Access

- External support that requires access can only do so by an approved connection method that requiresa unique username and password that will change on the next connection.
- Any access must always be monitored by a member of the ICT team until the access has expired.

Transfers and Disposals.

- Where a computer is to be transferred from one user to another ICT Staff are responsible for ensuring that data is transferred to the new computer and once verified and to ensure that it has been deleted from the old machine.
- Where a computer is to be sold, loaned, or donated outside of the Group, ICT Staff must ensure that the hard disk has been reformatted and the operating system reloaded to minimise the risk of data recovery.

Review

- This was reviewed in February 2022 and will be subject to review in February 2023.