This policy is issued to ensure that best practice is maintained so that the likelihood of a security breach through hacking, interception or other means is kept to a minimum.

1. Password Security

- Passwords will always be allocated by an authority appointed by the Information Security Management Representative;
- They will be allocated to a specific individual for their access only to the identified system;
- They must not be shared with anyone else.

2. Good Practice

- Each member of staff will have a unique password for the system(s) that they access;
- All computers will have a screen saver password activated within 15 minutes which will log the computer off;
- Passwords will be locked when employees leave the company;
- If a password must be written down it must be written only in an encrypted form so that no-one but the writer can determine what the password is;
- Passwords will not be displayed on the screen as they are entered;
- Temporary passwords will remain in use for the absolute minimum of time;
- In there is a suspected breach of password use the incident must be reported and logged as required in the company incident reporting procedures;
- Passwords will be a minimum of eight characters, at least one of which should be a numeric character and at least one special symbol and one Uppercase character;
- There will be no correlation between the password and the system being entered;
- No elements of the password will relate to the user (family names, nicknames etc.).

3. Password Maintenance

- Passwords will be changed regularly (minimum: every 6 months);
- Re-use of passwords is not permitted within 2 years;
- In the case of a suspected breach, the password will be changed immediately;
- Password software will require the entry of the old password before the new one is entered and accepted;
- New passwords will need to be entered twice;
- Password data will be held in encrypted format whether held electronically or otherwise.

Signed: _____ dated 15/1/19

Director