QRS Password Policy

Overall definition: QRS Password Policy for network access and files containing sensitive information (Full time staff)

Aims of the policy: `This policy is for full time staff who have access to the main QRS file server and may receive files containing information relating to individuals which needs to be kept secure.

Password Requirements:

- Must be a minimum of 9 characters.
- Must use at least 3 of the 4 following types of characters: upper case letter, lower case letter, numerical digit, special character.
- Prohibition of words found in a dictionary or the user's personal information.
- No more than 2 consecutive characters can be the same.
- Prohibition of passwords that match the format of calendar dates, telephone numbers, or other common numbers such as license plates.
- Prohibition of use of company name or an abbreviation.
- Never use the same password for a different client.
- Never use the same password twice for logins.
- Passwords must never be written down or stored under circumstances by members of staff other than by the IT Manager.

Administrator Procedures:

- It is the role of the IT Manager to make all members of staff aware of the procedures on setting and using passwords and making sure that this policy is being adhered to.
- Individual network passwords will be set by the IT Manager.
- Passwords for all PC's are automatically reset every 90 days or as soon as a member of staff leaves, or if it is deemed that there has been or is a potential for a security breach – which ever comes soonest.

POLICY REVIEW

This policy is reviewed annually.

These policies supplement your terms of employment but are not of contractual effect. Their purpose is to explain the Company's current policies and procedures, but they may be subject to change without notice if changes are considered appropriate by the Company or if there are changes in relevant legislation.