Acceptable Usage Policy

This Acceptable Usage Policy covers the security and use of all information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all employees, contractors and agents (hereafter referred to as 'individuals').

Computer Access Control – Individual's Responsibility
Access to the IT systems is controlled by the use of User IDs, passwords and/or pin numbers. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the IT systems.

Individuals must not:

- Allow anyone else to use their user ID and password on any IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-authorised device to the network or IT systems.
- Store data on any non-authorised equipment.
- Access websites that are inappropriate.

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Internet Conditions of Use
Use of the internet is intended for school purposes only. Personal use is permitted where such use does not affect the individual's school performance, or breach any terms of this policy. All individuals are accountable for their actions on the internet
.

Signed…… Date……