# Information Technology Acceptable Use Policy

Access to the school's Information Technology resources, including email and Internet access is for educational purposes only.  Inappropriate use of the Internet or other IT resources may result in a permanent or temporary ban on Internet and/or computer use.  The Relationships and Behaviour Policy and the Anti-Bullying policy will also be applied.

**Online Privacy**

Circulating, publishing or distributing (including on the internet or by other electronic devices) material associated with school activities  including but not limited to material in relation to staff and students  where such circulation undermines, humiliates or causes damage to another person is considered a serious breach of school discipline and may result in disciplinary action. As part of such disciplinary action the Board of Management reserves the right to suspend or expel a student or students where it considers the actions to warrant such sanctions.

This policy is devised in line with the Child Protection Guidelines as set out in the school's Child Protection Policy to ensure the safety of all students and in line with the Department of Education and Skills Child Protection Procedures for Primary and Post Primary schools.

**Scope of Policy**
This policy applies to all users of the school's information technology resources.

**Adherence to the following policy is necessary for continued access to the school's IT resources**:

**All users must** -

1. Respect and protect the privacy of others.
   o Not access, view, use, or copy accounts, passwords, data, or networks to which they are not authorized.
   o Not distribute private information about yourself or others.
2. Respect and protect the integrity, availability, and security of all school IT equipment including the network.
   o Observe all IT procedures, as posted.
   o Report security risks or violations to the network administrator and/or a teacher.
   o Not delete, destroy or damage data, networks, or other resources that do not belong to them.
3. Respect and protect the intellectual property of others.
   o Not infringe copyrights (not make illegal copies of music, games, movies, programmes or apps).
   o Use internet information and other IT resources for research, not directly copy or plagiarize.
4. Respect and practice the principles of the school community.

- o   Communicate only in ways that are kind and respectful.
- o   If a student unexpectedly comes upon any illegal and/or harmful images and text; whether violent, hate-based, or of a sexual nature, the supervising teacher must be told **immediately**. Under no circumstances should such material be revisited or downloaded.
- o   Users must not use school IT equipment to violate the school's rules of conduct or commit an illegal act.  This includes creating, accessing, copying or transmitting violent, threatening, rude, discriminatory, harassing, embarrassing images or messages; pornography; illegal copies of copyrighted works; stolen materials
- o   Users must not send spam, chain letters, or other mass unsolicited mailings.

5.   Take responsibility for their own work
- o   Users must copy and back up their own work. Data stored on the school network or PCs may be deleted by IT administrators at any time and may not be recoverable.

**Consequences for Violation**.  Violations of this policy may result in disciplinary action, including the loss of a user's privileges to use the school's information technology resources. Violations will also be reported to the appropriate authorities.

The school's Relationships and Behaviour Policy and Anti-bullying Policy also apply to any violations and will be followed and sanctions will be applied in line with those policies.

**Supervision and Monitoring.**  School and network administrators and their authorized employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property.  They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.

This policy was adopted by the Board of Management of Newpark Comprehensive School at its meeting of

12th December 2012.                           Date of next Review of this Policy: 12th December 2014

Signed: _____ Chairperson, Board of Management  Date_____

Signed: _____ Secretary, Board of Management     Date_____