Newpark
Comprehensive School
Scoil Chuimsitheach
Na Páirce Nua

Information Technology Acceptable Use Policy for Students

Newpark Comprehensive School recognises that access to Information Technology (IT) gives students enhanced opportunities to learn, engage, collaborate, communicate and develop skills that will prepare them for many aspects of life. To that end, the School provides access to IT for student use. This IT Acceptable Use Policy outlines the guidelines and behaviours that all students are expected to follow when using school technologies, whether in school or off-campus. This policy is devised in line with the School's *Relationships and Behaviour Policy*, *Child Safeguarding Statement*, *Anti-Bullying Policy* and *Mobile Phone Policy* and in accordance with the *Child Protection Procedures for Primary and Post Primary Schools 2017*. This policy applies to all student users of the School's IT resources.

Students are provided with a school email and password, which allows access to the Microsoft Office 365 platform of applications (Outlook, Teams, OneNote, Word, Excel, PowerPoint etc).

- The School IT platform is intended for educational purposes only and school related conversations only. It is not a space for social media activity.
- All activity in Office 365 may be monitored and retained.
- Students should not use a personal email for school activity, or a school email for personal activity. School emails should not be forwarded to personal email accounts.
- Students should ensure their password is known only to them.
- Students are expected to follow the same rules for good behaviour and respectful conduct online as offline. These rules can be found in the School's *Relationships and Behaviour Policy*.

Cyber-bullying

Cyber-bullying is not tolerated. Harassing, impersonating, outing, tricking, excluding and cyber-stalking are some examples of cyber-bullying. Cyber-bullying may be deemed a crime. Students should remember that all online activities are monitored and retained. The School will support students, teachers and parents/guardians in responding to cyber-bullying. The School is committed to the *Child Protection Procedures for Primary and Post-Primary Schools 2017* and will act as required by the Department of Education, the Department of Children and Youth Affairs, the Department of Justice and Equality and the Health Service Executive.

Content Filtering

Content filtering is an essential and integrated element of the broadband service that is provided to schools by the *Schools' Broadband Programme*. The purpose of content filtering is to ensure, in so far as is possible, that inappropriate websites and content are not accessible within schools. For this reason, students are only permitted to use and access the student Wi-Fi. Other Wi-Fi networks are not permitted. The School's chosen level is number 5 Content Filtering. This allows access to millions of websites and allows access to 'personal websites category' and other similar types of websites, such as blogs, but does not allow access to social networking sites, such as 'SnapChat', 'Instagram', 'TikTok' etc.

Adherence to the following is necessary for continued access to the School's IT resources:

1. Respect and protect the privacy of others.
   - Users should avoid accessing, viewing, using, or copying accounts, passwords, data, or networks to which they are not authorized.
   - Users should not distribute private information about themselves or others.

- Users must not take, use, share, publish or distribute images of others without their permission.
- Users must not share images, videos or other content online with the intention to harm another member of the school community, regardless of whether this happens in school or outside.

2. Respect and protect the integrity, availability, and security of all school IT equipment.
    - Observe all IT procedures and protocols for using school IT equipment.
    - Users must report security risks or violations to the network administrator and/or to a teacher.
    - Users must 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.
    - Users must ensure that when using internet information and other IT resources for research, that they are not copying or plagiarizing. Research conducted via the Internet should be appropriately cited, giving credit to the original author. Use of Artificial Intelligence (A.I.) for schoolwork is strictly prohibited.
    - Users should not infringe copyrights.

4. Respect and practice the principles of the School community.
    - Users should always only communicate in ways that are kind and respectful.
    - Cyber-bullying will not be tolerated. Refer to the School's *Anti-Bullying Policy*.
    - 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, downloaded, photographed or shared.
    - Users must not use the School's IT system to violate the School's *Relationships and Behaviour Policy* or commit an illegal act. This includes creating, accessing, copying or sharing rude, embarrassing, threatening, discriminatory, harassing, or violent images or messages; pornography; illegal copies of copyrighted works; stolen materials.
    - Users should endeavour to observe the recommended 6pm cut-off time for School communication.

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 system. 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 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 users are secure and in accordance with this policy. Administrators reserve the right to examine, use, and disclose any data found on the School's information networks to further the health, safety and well-being 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 authorities. Internet safety and acceptable online behaviour is taught within the School's Junior Cycle wellbeing programme.

This policy was reviewed in the 2022/2023 academic year and will be reviewed again as required going forward, in line with changing information, guidelines, legislation and/or feedback from school stakeholders.

This policy was ratified by the Board of Management, Newpark Comprehensive School at its meeting on 26th April 2023.