Nottingham High School IT Acceptable Use Policy for IT [students]

THIS POLICY REFERS TO ALL PUPILS INCLUDING THOSE IN EYFS

IT Acceptable Use Policy for IT [students]

Contents

IT Acceptable Use Policy for IT [students]

1. Policy Statement

General principles

The School wishes to teach students and inform parents of the benefits of IT and Internet access to students and, at the same time, advise students and parents of the potential for misadventure which may result from access to the network and Internet. In providing Internet access for students, the School commits itself to providing e-safety training so that students learn to use the Internet in a mature and responsible way.

The Internet provides access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages, for example. The filtering system used in our school blocks inappropriate content. We currently filter out several social media sites, such as Facebook and Twitter. Searches and web addresses are monitored and the IT technicians will alert senior staff where there are concerns and prevent further access when new sites that are unblocked are found.

Although students have unfiltered internet access when using their mobile phone or other personal device on a non-school internet connection (3G/4G/5G), this policy still applies to the use of those devices in school.

In order to ensure the security of the computer network and the health and safety of students, the school will exercise its right by electronic means to monitor the use of the computer systems and network. This includes, but is not limited to, the monitoring of:

- Search Terms,
- web sites visited,
- printer usage,
- interception of email,
- the deletion of inappropriate materials, and
- the storing of text, imagery or multimedia files which are unauthorised or unlawful.

This policy should be read alongside the Online Safety Policy and behaviour policies.

2. Network Acceptable Use

The policy below applies at all times, in and out of School hours, whether the school facilities (including cloud services) are accessed directly or from a remote location. Students and parents are asked to read the policy carefully before signing the "Nottingham High School IT Student Registration Form".

IT Acceptable Use Policy for IT [students]

In clarifying the acceptable uses of the network, the following is a list of guidelines and a list of specific behaviours which are unacceptable and that may lead to School disciplinary action and/or suspension or limitation of School network and Internet access privileges:

1. When interacting with other users on the network or Internet, users are expected to behave as they would in any other environment where they represent the School. It is important that users conduct themselves in a responsible, ethical, and polite manner in accordance with the standards expected of a member of Nottingham High School.
2. The School's networks are intended only for educational purposes and for the business and administrative functions directly in support of the School's operation.
3. Network services, and access to these services, shall only be used by authorised persons.
4. Using the School's networks and the Internet for illegal, obscene, harassing or inappropriate purposes, or in support of such activities, is prohibited.
5. Intentional damage will result in disciplinary action and you may be billed for repairs or replacement.
6. All above rules apply whether School network access is gained from in or out of school settings.

All users are required to comply with the following:

1. Users may not use the School's networks or computing equipment to:

    - transmit any materials in violation of UK laws.
    - duplicate, store, view or transmit pornographic materials.
    - transmit or post threatening, abusive, obscene or harassing material.
    - duplicate, store, or transmit copyrighted material that violates copyright law.
    - Share or forward any confidential information.

2. Users may not violate, or attempt to violate, the security of the School's computers, data or network equipment or services.

    - Any attempts at unauthorised access of School data may result in termination of the user's computer and network privileges.
    - Any attempt to vandalise School network accounts or systems may result in termination of the user's computer and network privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another member, the School, or any of the agencies or other networks that are connected to the Internet. This includes, but is not limited to, the uploading or creation of computer viruses.
    - Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the School's networks and services.

3. Users may not:

- use abusive, vulgar, profane, obscene, harassing, or other inappropriate language;
- bully others using technology ("cyber-bullying"). This includes, but is not limited to, prank telephone calls, sending unpleasant text messages or images/videos, posting on hate sites, forwarding or sending inappropriate emails;
- share password(s) with others. Where password-protected accounts are used, network users are personally responsible for all activity that occurs within their account;
- distribute or use anyone else's account name and password;
- reveal anyone else's personal address, phone number, or picture;
- use network access for business purposes or anything else not related to the individual's position in the School;
- eat or drink near any machine or in any of the IT Centres;
- play online games during lesson times unless they contain educational content and have been authorised by a member of staff;
- Connect personal devises to any school network (Hard Wired, or Wi-Fi) other than the BYOD Wi-Fi network.
- Live stream any content from school premises or whilst on any external school activities.

3. Internet and Email Acceptable Use

Internet use is for educational based work only.

Students must:

- Comply with any applicable laws, including the Computer Misuse Act, Data Protection Law, Copyright, Design & Patents Act and The Telecommunications Act.
- Note that entering into illegal or offensive activity is strictly banned (including sharing such information).
- Report any unblocked inappropriate content (e.g. extremist) to a senior member of staff

Students must not:

- Attempt to bypass the school security in any way by using 'Proxy Avoidance' sites, VPN's or attempt to get around the School's blocking/filtering systems.
- Download files such as executables, movies or music files (mp3s) or run any program which has not been authorised.
- Attempt to use Peer to Peer sites, or any other unauthorised utility.
- Make purchases via shopping, auction sites.
- Use your school email address or school facilities for mass emailing or spamming.

Please note:

- Nottingham High School accepts no responsibility for the malfunctioning of any IT facility or part thereof, whether hardware or software, nor for any consequential losses. Backups are made every evening but the user is responsible for independently maintaining copies of valuable data.

Nottingham High School reserves the right to modify this Acceptable Use Policy for IT, as appropriate. Changes will be published on the School website.