Acceptable Use Policy

This document provides advice and guidelines, and specifies activities prohibited by Norfolk County Council (NCC) to anyone using the Norfolk Schools' Network (hereinafter referred to as 'the Service') for Internet access.

This policy is part of the Internet Access Agreement between NCC and any school. For the purpose of this document, the term "Computing Subject Leader" also refers to any member of the school staff with specific computing responsibilities.

Policy

1. General Information

1.1 NCC reserves the right to monitor the use of the Service and, if necessary, to temporarily disconnect any site from the Service when exceptional circumstances dictate that such action is necessary to safeguard the integrity and performance of the Service.

1.2 Use of the Service for unlawful purpose or activity may require NCC to co-operate and assist the police or others with their investigations.

1.3 NCC is unable to exercise control over and has no responsibility for information passing over the network.

1.4 School staff must be continuously aware of (and exercise vigilance to safeguard against) the potential for Internet access to information or content that may be inappropriate or unsuitable for younger age groups and certain other users, and that this information is beyond NCC's control.

1.5 No Item to be bought into school without prior permission of the head teacher.

2. Using the Service

Users should not use the service:

2.1 In any way that constitutes, or is associated with a criminal offence.

2.2 In any way that is contrary to NCC Personnel Guidelines; this will also include access to and use of social networking sites.

2.3 To infringe the copyright or intellectual property rights of any other person or body.

2.4 To circumvent user authentication.

2.5 In any way that adversely affects the level of service to any other user.

2.6 To send any type of electronic communication with the intention of adversely affecting the performance or functionality of any computer or networking system.

2.7 To host Internet services or provide external access to third parties for commercial gain.

3. Excessive Use

3.1 The Service is a shared resource and its users should avoid making excessive use of the Service to the detriment of others.

Examples of excessive use include, but are not limited to:

- Streaming video continuously
- Streaming audio continuously
- Video/audio conferencing continuously.

3.2 NCC will monitor the service traffic and users making excessive use will be informed and requested to reduce their usage, unless exceptional circumstances apply.

4. Security

4.1 Users must not use or attempt to use the Service without authority to:

- Gain access to or use data, systems or networks
- Probe, scan or test the vulnerability of a system or network
- Breach system or authentication measures
- Monitor data or traffic
- Carry out any other activity that could be detrimental to the security and / or performance of the network.

4.2 Users must not interfere with the service to any other user, host or network. Examples of such interference include, but are not limited to, mailbombing, flooding and deliberate attempts to overload the system.

5. Password Management Guidelines

5.1 Passwords/user logon IDs must be unique to each user

5.2 Passwords should consist of a minimum of 6 alphanumeric characters (no names or phrases that might identify the user)

It is accepted that passwords of less than 6 characters are likely to be more practical for younger age groups

5.3 Passwords must be kept private**.**

6. Virus Prevention, Detection and Removal

Many systems contain data and applications that are critical to system owners. Infection will cause considerable loss of time and data and will have serious detrimental impact for curriculum activity. Large numbers of computers may be involved and all reasonable measures possible must be taken to prevent virus infection.

New viruses and more sophisticated viruses are being developed constantly. Therefore, ant-virus software must be updated on a not-less-than weekly basis to maintain currency with the latest viruses.

Users should be instructed to inform the Computing Subject Leaderr of any different or out-of-the-ordinary behaviour a computer or application exhibits.

To reduce the risk of spreading a virus, a computer must be disconnected from networks immediately it is known or thought to be infected.

6.1 Virus Prevention:

6.1.1 Users must be kept informed about the possibility of receiving viruses and other malicious code from the Internet.

6.1.2 User training must include information about virus infection risks and how viruses can be spread.

6.1.3 Anti-virus software must be installed and running on all file servers and computers including laptops.

6.1.4 Scanning of all files and executables must occur frequently (e.g., daily) on the file servers.

6.1.5 Anti-virus software must be configured to scan data as it enters the computer.

6.1.6 Anti-virus scanning tools must be used to scan computers weekly.

6.1.7 The service offers safe and secure access to the Internet and downloads occurring outside this protected environment, e.g. at home, should be considered a probable source of virus infection. For this reason, all laptops must be virus-checked before being connected to a network.

6.2 Detection:

6.2.1 Immediately a virus has been detected, the Computing Subject Leader must inform ICT Shared Services of the circumstances and take steps to prevent further infection (multiple phone calls about the same virus should be avoided as far as is practicable).

6.2.2 Computing Subject Leaders must be aware of the steps necessary to determine if their system is infected and the steps to take to remove the virus.

6.2.3 All data imported on to a computer (e.g., via disk, e-mail, or file transfer) must be scanned before being used.

6.3 Removal:

6.3.1 To reduce the risk of propagation, any computer thought to be infected by a virus must be disconnected immediately from all networks and quarantined.

6.3.2 Infected computers must be disinfected in accordance with anti-virus software manufacturers' recommendations.

6.3.3 Infected computers must not be reconnected to the network until the Computing Subject Leader verifies that the virus has been removed.

Ratified by Governors on 15th November 2018

Chair of Teaching and Learning Committee________________________