Strathearn School

Acceptable Use of the Internet

Acceptable Use of the Internet at Strathearn School

To all pupils, parents/guardians and staff

Contents

1   Introduction

As part of the school's curriculum, we offer pupils access to the Internet reflecting its increasing use in our society in general.

The Department of Education provides schools with the necessary hardware, software and connectivity to enable access to the Internet through an organisation called C2k. Access is thus controlled through a filtering mechanism managed by C2k.

Websense assesses all websites based on their content and adds them to a category. Through the C2k service, categories of sites can be made available to users, while access to other categories will be restricted. Access to the most inappropriate sites, including those on the Internet Watch Foundation banned list, will always remain blocked.

Note: The same C2k filtering applies across the C2k network, whether using a C2k core desktop computer or a personal iPad. This consistency is essential to ensure the safety and integrity of C2k's internet provision. Internet activity is logged so historical records can be investigated if required.

However, no matter how thorough, a filtering service can never be comprehensive. It is possible for unsuitable websites to become available, sometimes for short periods after they are launched. As soon as a site is deemed to be unsuitable, it will be blocked, so that no user can subsequently access it.

Families should be aware that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive.

Whilst our aim for Internet use is to further educational goals and objectives as identified in Departmental Schemes of Work, pupils may find ways to access other materials as well. Ultimately it is the joint responsibility of school staff and the parent or guardian of each pupil to educate the pupil about their responsibility when using the Internet.

Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, books, movies, radio and other sources of potentially offensive media.

2   A Brief Guide to the Internet

The Internet

The Internet is a large number of computers all over the world linked together through cables and telephone lines. In most cases, each of these computers is also linked to a number of other computers, in a local network.

It is possible for someone using one of these computers to gain access to information on any of the others. It is also possible for other people, outside these local networks, to connect to the Internet by using standard telephone lines between their computers and those already connected to the Internet. Most schools, including Strathearn, have their own website. Strathearn's website may be found at http://www.strathearn.org.uk.

Electronic Mail (Email)

This is a way of sending messages from one person to another via the Internet. Each Strathearn pupil and member of staff with a C2K account have an email address.

The C2k email system is protected by Websense filtering solution which safeguards staff and students from viruses, spam and inappropriate content. The software is continually being evolved in response to feedback and to take advantage of technological advances.

The filtering policy will automatically analyse each message according to the criteria defined below and block if appropriate.

- Image Analysis (inappropriate or unrecognised images);
- Textual Analysis (inappropriate language);
- Media/file type not recognised;
- Attachments with executable programs;
- Virus detected;
- Spam;

The message will then be treated in one of the following three ways:

Delivered:	The message is delivered
Held:	Pupils do not have this facility. Affected staff members may release held messages by requesting a message report to their school email address from: https://admin.websense.net/utility/message_report.mhtml Or by logging a call with the C2K Service desk 0870 601 1666
Not held or delivered:	The message is not delivered to the mailbox and is not available for release.

What *are the dangers of the Internet referred to in the media?*

It is true that there is some material on the Internet that would be offensive to most people, such as pornography, racist and fascist material, and it is possible for children to find access to this.

Electronic filter systems aim to prevent access to inappropriate material; however, such technical efforts are unlikely to be completely effective.

An alternative approach is to educate our pupils and encourage acceptable use through partnership between home and school in dealing with the less savoury side of Internet use.

Social Media / Messaging Services

Social networking sites and apps, e.g. Facebook, Twitter, WhatsApp, SNAPCHAT, Yellow, TikTok, Omegle, askfm (this is not an exhaustive list) are very popular but are also open to abuse by adults posing as children. Although these services cannot be accessed from within school, it is possible for children to access them from other places. In order to try to protect our pupils we endeavour to educate them about the dangers of these activities at all levels.

Further advice can be found on the Childnet website at www.childnet-int.org and on the Child Exploitation and Online Protection (CEOP) Centre's website www.thinkuknow.co.uk .

3   The School Rules for Internet Use

Pupils are responsible for good behaviour on the Internet just as they are in a classroom or a school corridor. General school rules apply.

The Internet is provided for pupils to conduct research and communicate with others. Access is a privilege, not a right and access requires responsibility.

Individual users of the Internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with school standards.

Pupils who access Internet sites, apps and platforms using their own data network and through their own personal device whilst in school do so at their own risk and must ensure they act within the limits for mobile phone use set out in the Positive Behaviour Policy.

Staff can inspect files in computer storage areas to ensure that users are using the system responsibly. Users should not expect that files stored on servers or disks would always be private.

The following list outlines some of the behaviours which are not permitted:

1   Using others' usernames and passwords;
2   Trespassing in others' folders, work or files;
3   Harassing, insulting, bullying or attacking others;
4   Creating, displaying or sending offensive messages or pictures;
5   Using obscene language or content;
6   Damaging computers, devices, peripherals, computer systems or networks;
7   Cheating in exams/assessments by accessing information through an internet enabled device;
8   Violating copyright laws;
9   Transmitting copyrighted materials;
10   Intentionally wasting limited resources;
11   Stream video or audio i.e. live radio when not part of a taught lesson or instructed homework;
12   Use another's allocated device or type on another's keyboard during class;
13   Playing Games on the iPad, Chromebook or school workstation during class time without permission;

Violations of this policy will result in sanctions in accordance with the Positive Behaviour Policy

The above examples of misconduct are not exhaustive. The Principal reserves the right to decide how any other example of misconduct will be dealt with.