



## **Acceptable Use Policy - Students**

**Status:** Additional

**Purpose:** To promote e-safety and protect students from undesirable materials on the Internet, undesirable contacts and other dangers associated with the Internet, to endeavour to ensure all school data is stored securely, and to prevent unacceptable use of the ICT systems.

### **Links to other policies:**

- Standards for Learning - Behaviour
- Anti – Bullying
- Child Protection
- Disciplinary Procedure
- E-Safety Procedure

### **Definitions:**

#### *Undesirable materials*

- Pornographic images or obscene text
- Language that is abusive, profane, inflammatory, coercive, defamatory, blasphemous or otherwise offensive
- Images, videos, text or other materials that are used for the purpose of Cyberbullying
- Racist, exploitative or illegal materials or messages

#### *Undesirable contacts*

- E-mail messages from unknown or unverified parties, who seek to establish a person's identity and/or to communicate with them, such as for advertising or potentially criminal purposes.
- Electronic contact between staff and students/parents must remain within the school's ICT systems (i.e email or VLP) and should be of a professional nature.
- Staff communication with current students and/or family members of those students via social networking sites (e.g. Bebo, MySpace, Facebook, Twitter, etc.) is strictly prohibited

#### *Unacceptable use*

- Deliberate searching for, and accessing of, undesirable materials
- Instant messenger / chat rooms
- Creating and transmitting e-mail messages that contain unacceptable language or content
- Creating and publishing on the Internet or School system materials that contain unacceptable language or content
- Downloading, installing, reconfiguring or removing software of any kind without the express permission of the Headteacher or a member of the ICT Technical Team
- Accessing the School's ICT system or Internet via any username or password other than that provided to you by the school
- Accessing and/or playing non-educational games

#### *Unacceptable use unless related to educational needs*

- Copying or downloading video or music onto the School's system from the Internet, network or removable media (eg. Portable MP3 players, USB devices, optical media)
- Sharing, copying or removing files via the School network without the express permission of a member of staff
- Accessing and/or playing educational games unless directed by a member of staff

#### *Copyright breach*

The downloading, copying or transferring of copyrighted material, such as music and video content and other digital resources, without the express permission of both the School and copyright holder is expressly prohibited.

### *Students*

Children of school age that are either members of the school or visitors from another school. The staff member responsible for the visiting students should ensure that they are aware of the school's policies prior to granting them access to the school's ICT systems.

### **Implementation:**

*Promoting e-Safety* – Students are encouraged to keep passwords confidential and user accounts secure by frequently changing passwords and therefore protecting their documents and user areas from inappropriate use by others. Students should log out of accounts when leaving their workstation and never leave a logged in account unattended.

*Investigating ICT usage* - ICT usage will be routinely monitored with suspect usage investigated accordingly. This will include the review of Internet access, user space content, the content of shared areas and email accounts accessed by students. The School reserves the right to remove any material stored on its systems and request the removal of any material held by a third party that relates to the School, its community or its practices.

*Unintentional Exposure of Users to Undesirable Materials* - every reasonable step should be taken to prevent the exposure of users to undesirable materials on the Internet. It is recognised that this can happen not only through deliberate searching for such materials, but also unintentionally when a justifiable Internet search yields unexpected results.

To prevent such occurrences, the School has adopted the following position:

- Content Filtering System (Websense) which offers protection by the imposition of a "banned list" of undesirable sites. This list is updated daily and the school can make further additions to the list.
- The filtering of sites by a site grading process.
- The filtering of sites by language content with prohibition of sites with unacceptable vocabulary.
- The filtering of all `Newsgroups`, chat rooms and forums considered to be the most unacceptable area of the Internet. This does not include those hosted on the school's systems such as the Virtual Learning Platform.
- The detection and filtering of inappropriate images and videos using ScreenShield which detects flesh tones and replaces suspect content with a warning image.
- The detection and capture of inappropriate language using Policy Central which detects key words and stores a screen capture which can be used to filter inappropriate content and websites as well as effectively tackle occurrences of Cyber-bullying.

In-school we are able to offer further protection by:

- Adult supervision of students' Internet activity during lesson time. Adult supervision and surveillance by staff in the vicinity of students' Internet activity at lunchtimes and other non-teaching time.
- The "caching" of Internet sites in advance by staff so that students work off-line and are not able to browse.

In the event of students being unintentionally exposed to undesirable materials, the following steps will be taken:

- Students should notify a member of staff immediately
- The member of staff will notify either Head of ICT or ICT Manager
- The source of the material will be investigated and dealt with appropriately
- Parents and/or Governors will be notified at the discretion of the Head according to the degree of seriousness of the incident

*Intentional Access of Undesirable Materials by Students* - Students must never intentionally seek offensive material on the Internet. Any transgression will be reported and dealt with as follows:

- Staff member will report incident to Head of ICT and ICT Manager
- Access to the students account will be locked immediately and an investigation carried out
- The e-safety procedure will be followed and if a child protection issue is identified it will be reported immediately to the Child Protection Officer
- Details of the incident and any findings will be recorded
- The incident will be treated as a disciplinary matter, and the parents and appropriate staff will be informed

If deliberate access to undesirable materials is found to be repeated, flagrant or habitual, the matter will be treated as a serious disciplinary issue.

*Receipt and transmission of E-mails by Students* - E-mail messages received or transmitted by students can contain language or content that is unacceptable. It is also recognised that some people may try to use e-mail to identify and contact students for unacceptable reasons.

To avoid these problems the School has adopted the following practice:

- As part of the ICT curriculum students are given an explanation of the dangers of e-mail and advice upon its usage
- Steps may be taken to verify the identity of any entity or person seeking to establish regular e-mail contact with the School or its community
- Students are aware that e-mail messages may be audited and are not guaranteed to be private
- Students are encouraged not to reveal their full names or addresses. Similarly, information is never given that might reveal a pupil's whereabouts.
- If staff believe that students have been targeted with e-mail messages by parties with criminal intent, the messages will be retained, the incident recorded, and appropriate steps taken

*Publishing of Materials on the Internet* - students may at some time produce and publish materials on an Internet Web Site associated with the School. No materials will be published on the Internet which contains any unacceptable images, language or content. Infringement of this rule will be taken as a serious disciplinary issue.

In publishing material on the Internet the school will take steps to ensure that student identities are protected at all times. The publishing of material on the Internet relating to the School, its community or practices is strictly prohibited, unless the website is owned or managed by the school, and may result in legal action if not removed upon request.

The publishing of material on blogs, forums, personal social networking sites (e.g. Bebo, MySpace, Facebook, Twitter, etc.) or media content sites which directly relates to the School, its community or practices and which is deemed to be of a derogatory nature is prohibited and may result in disciplinary action or prosecution.

#### *Copyright Issues*

It is recognised that all materials on the Internet are copyright, unless copyright is specifically waived. It is the school's policy that the copyright of Internet materials will be respected. Students who are unsure about matters of copyright should seek advice from a member of staff.

#### **Monitoring and Evaluation**

- Incidents will be reported to HBC using the 'Caldicott Incident Monitoring Form' as soon as possible after any breach of this policy
- A record of any abuse will be kept by the Head of ICT and ICT Support.
- A written report of incidents will be submitted to the Senior Leadership Team on half termly basis.
- A written report will be submitted to the Governing Body on a termly basis.

**Policy written by:** M Draycott, ICT Manager  
K Holland, Subject Leader, ICT

**Date adopted by Governors:** March 2010

**Date for review (bi-annual):** Summer 2010/Winter 2011