

## INTERNET ACCEPTABLE USE

*Last update – November 2010*

### Educational Purpose

The KLB Network/Internet access has been established for an educational purpose. The term "educational purpose" includes classroom activities, career development, quality research activities, administrative and business support for the work of the school.

### Scope of this policy

This policy applies to:

- all members of the school community when they are using computer equipment which is the property of the school and any internet access on the school site;
- external contractors or other visitors if they are granted temporary use of the school's equipment or when they use their own equipment on the school site;
- the use of laptop computers which are the property of the school when they are used to access the internet away from the school site;
- computers and other devices which may access the internet on the school site through alternative connections, for example the mobile telephone network.

### Use of Internet facilities

The school Internet service is provided by the South West Grid for Learning (SWGfL). The SWGfL monitors and audits the use of the Internet by KLB School and reports any potential misuse that it identifies. If inappropriate material is accessed accidentally, staff users should immediately report this to another member of staff so that this can be taken into account in monitoring. The School expects all users to use the Internet responsibly and strictly according to the conditions listed below.

### A summary of unacceptable usage:

Members of the school community will not use any school equipment, computers or Internet access service to:

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - pornography (*including images, video as well as explicit animation and textual descriptions*);
  - graphic portrayal of violence (*other than as is necessary to support a course of study in the school curriculum appropriate to the age of the children involved*);
  - promoting discrimination of any kind (*including material that promotes intolerance on the basis of gender or sexual orientation*);
  - promoting racial or religious hatred;
  - promoting illegal acts;
  - promoting drugs and substance abuse (*Including web sites that promote the use, manufacture and distribution of illegal drugs, as well as sites that promote the abuse of legal substances such as prescription drugs or the sale of alcohol to minors*);
  - promote violence or self-endangerment, or contain instructions for making weapons of violence or the sale of such weapons,
- Access web-based chat sites that allow users to make contact with individuals in the outside world without, providing sufficient safeguards and protection to young people.
- Access social networking sites (such as Facebook, Bebo etc.)
- Access web-based email services, other than the service provided by the school.
- Access sites offering Internet-based SMS messaging services.
- Run any form of private business or create, edit or access their own web pages outside the school network or approved school web sites.
- Visit sites that might be defamatory or incur liability on the part of the school.
- Upload, download, or otherwise transmit (*make or distribute*) commercial software or any copyrighted materials belonging to third parties outside the school.
- Reveal or publicise confidential or proprietary information, which includes but is not limited to: financial information, personal information, database content, computer/network access codes

and business relationships.

- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (*sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion*) that substantially hinders others in their use of the Internet or school network.
- Solicit, represent personal opinions or reveal confidential information or use it in any other way that could reasonably be considered inappropriate.
- Carry out political lobbying, either directly or via email, excluding the use of the system to communicate with elected representatives and express opinions on political issues.
- Access the UseNet Internet News system or Chat services, e.g. IRC and ICQ.

## **Monitoring**

All access to the internet through the school's internet connection is logged. All pupil access is also filtered. Attempts to by pass the filter are also logged. These logs are inspected on a sampling basis or when there is suspicion of unacceptable use. Staff are able to apply for unfiltered access to the internet in order to support specified curriculum related activities. Such unfiltered access is logged separately and checked on a sampling basis or when there is suspicion of use which does not correspond to the curriculum activity specified.

All email sent and received using the klbschool.org.uk domain is logged and filtered by SWGfL. As stated above, alternative web based email such as Hotmail should not be accessed through the school's internet connection.

When pupils use the internet, staff are expected to be vigilant to ensure that appropriate use is being made of the facility.

When laptop computers are checked by the IT technicians, the contents of the internet cache are inspected on a sampling basis to check that unacceptable internet sites have not been accessed using the equipment.

## **Sanctions for unacceptable use**

Pupils who make unacceptable use of the internet will be dealt with through the school's sanctions procedure according to the nature of the incident. Sanctions may include detention, exclusion and withdrawal of internet access for a specified period of time.

If a member of staff makes unacceptable use of the internet, the response will correspond to the nature of that use. The response could range from an informal warning to dismissal for gross misconduct. If necessary, the Gloucestershire Safeguarding Children Board and/or the police will be informed.

Associated policies:

Laptop acceptable use policy

Safeguarding Policy

Guidelines for safer working practice for adults who work with children and young people

Staff Conduct Procedure

*Approved by Governors: 8 December 2010*

*Date of next review: Autumn 2012*