



1. **Title:**

ICT Acceptable Use Policy

2. **Purpose:**

- To regulate use of the School's ICT facilities
- To establish the parameters of acceptable usage of these facilities
- To inform users of the arrangements for filtering web-traffic
- To inform users of the procedures for reporting abuse
- To inform users of sanctions that may be applied following misuse

3. **Aims:**

For Teachers:

- To establish the boundaries for acceptable professional use
- To alert them to issues that may impact on their classroom practice
- To highlight the e-safety issues associated with the use of ICT
- To inform them of the procedures for reporting misuse

For Students:

- To establish the boundaries for responsible use
- To help them identify issues that may impact on their learning
- To develop their awareness of e-safety
- To inform them of the procedures for reporting misuse

4. **Policy:**

- The School declares an interest in all ICT equipment used on the site for whatever purpose
- The School's ICT facilities are the property of the School and provided for educational use: any misuse will be treated as a disciplinary matter
- Only authorised ICT equipment and School-licensed software may be used on the School's network
- Where unauthorised equipment needs to be attached temporarily (eg for display purposes) the Network Manager must be consulted beforehand
- Users are responsible for the password security and the content of their assigned network area(s)
- Users should be aware that all School network usage is logged and monitored. Authorised staff may investigate suspected misuse of any part of the School's ICT facilities and present this as evidence for disciplinary action
- Where misuse contravenes legislation relating to the use of ICT equipment, the appropriate authorities will be informed and legal action taken
- Users are not permitted to download, install, run or distribute software applications of any description without the permission of the Network Manager

- Users may not use any applications or internet proxy services to circumvent the security of the School's ICT systems
- The School reserves the right to confiscate and investigate any piece of ICT equipment found on site that may be being used inappropriately, illegally or in a manner that would bring the School into disrepute
- All users are responsible for protecting the information on and passwords to any protected areas of the network to which they have access
- Users must not allow others to make use of their network account
- Users are responsible for ensuring that content stored on their network area does not infringe the laws of copyright

Internet Usage

Access to the internet is provided by The South West Grid for Learning via South Gloucestershire Council. Their Acceptable Usage Policies form the basis of the School's Policy.

The purpose of this Policy is to ensure that users understand the way in which the Internet is to be used. The Policy aims to ensure that the Internet is used effectively for its intended purpose, without infringing legal requirements or creating unnecessary risk. Users should read this Policy alongside the other School policies.

Scope

The Policy applies to:

All users and administrators of the School's ICT services and/or infrastructure. On evidence provided by the ICT support team or other member of the School's staff, a registered user may be disciplined by the School.

At the same time, if a user's conduct and/or action(s) are illegal, the user may become personally liable in some circumstances.

Policy statement

The School encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. It should not compromise the School's information and computer systems nor have the potential to damage the School's reputation.

Please read the Policy carefully as you will be deemed to be aware of its contents.

Use of Internet facilities

The School expects all users to use the Internet responsibly and strictly according to the following conditions:

For the purposes of this document, Internet usage means any connection to the school network or Internet via Web browsing, email or news groups.

Users shall not:

Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- any other information which may be offensive to other users

The School acknowledges that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use (for example investigating racial issues). Any such access should be preplanned and recorded so that it can be justified if required.

Incidents which appear to involve deliberate access to Web sites, newsgroups and online groups that contain the following material will be reported to the Police:

- images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative
- adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material in the UK

Filtering

The main filtering of internet content is provided by RM SafetyNet Plus, administered by the South West Grid for Learning. RM SafetyNet plus is designed to filter out material found to be inappropriate for use in the education environment.

The Web-based email services and mobile phones/SMS/ring tones filter lists are set to 'off' as default in RM SafetyNet Plus.

Material designed to educate, for example on matters such as sexual health or combating drug and substance abuse would not normally contravene the SWGfL's Internet filtering Policy.

A general benchmark used by RM/SWGfL to determine whether a site or part of a site should be filtered, is whether or not the questionable material is something which the national press may publish. If it is, then it is unlikely RM/SWGfL would choose to filter it.

RM/SWGfL block user-access to a huge number of unsuitable WWW sites. This by the exclusive method, which means that when an inappropriate Web site is found, RM/SWGfL prevents user access to it. This is as opposed to the inclusive method, which restricts access to all Web sites, except those identified as appropriate.

Although it would be impossible to identify all unsuitable Web sites, SWGfL believe that the exclusive method is the most suitable Internet Filtering Policy. Essentially, they believe that the majority of their customers would find the

inclusive method too restrictive, as the scope of acceptable sites would be too limiting.

In addition RM SafetyNet Plus utilises Content Filtering technology. This technology dynamically scans pages requested for inappropriate content. The content filter may filter pages that have not yet been added to an RM/SWGfL filter list, providing an additional safety check.

Custom Filtering

The School can identify sites it feels are appropriate for its educational purposes and RM/SWGfL may choose to unfilter them. In the event that this is refused, the School has its own custom filter list to enable these sites to be unfiltered. Conversely, unfiltered sites deemed to be undesirable by the School can be filtered using this technology.

Beyond the World Wide Web

In addition to the World Wide Web, the SWGfL has identified a number of key areas of the Internet that contain a significant degree of controversial material:

- The UseNet Internet News system
- Chat services, eg IRC and ICQ

UseNet

The UseNet system comprises of more than 40,000 discussions groups, which cover a huge range of topics from the Beatles to Star Trek and from needlework to UNIX.

Some of the UseNet groups contain material which is likely to cause offence. Such messages are normally contained within easily identifiable groups such as alt.sex.stories, but there is no guarantee that any group won't contain an occasional offensive posting. Note that UseNet messages can contain pictures or sounds as well as text. The SWGfL prevents access to UseNet, however should sites require access, this can be enabled through Change Control.

The SWGfL News services only carries newsgroups that are believed to be safe. In addition, the SWGfL restricts customer access to other news services so that users cannot easily circumvent the blocking.

Chat Services

After a considerable amount of feedback, the SWGfL has taken the decision to prevent access to the majority of Web-based chat services.

Like the WWW and UseNet, there are chat sites covering almost every subject, but they generally differ in a number of ways. Most chat services are run in real time, which means that the text typed in is visible by anyone else using the Web site at that point in time. There is also very little opportunity to regulate the content of the communications, which leaves it open to considerable abuse. What appears to be a perfectly innocent discussion could rapidly change direction. There is also the potential for personal information to

be disclosed, which is not necessarily appropriate for users who are, on the whole, under eighteen.

It is important to remember that users are unlikely to ever see the person that they are 'chatting' to and therefore there is no guarantee that a correspondent is the person they say they are.

For these reasons, SWGfL have blocked access to the majority of chat sites.

Not a 100% Guarantee

RM/SWGfL proactively conducts thorough searches in an effort to block user access to any inappropriate material. However, it is important to understand that the product can only decrease the likelihood of the customer or an end-user accessing inappropriate content but cannot guarantee that such content will not be accessed. One reason for this is the enormous size of the Internet and the fact that it is a continually changing environment, with new material added by the minute. Therefore it is imperative that if schools find Web sites of an inappropriate nature that the SWGfL is informed (via the filtering email: filtering@swgfl.org.uk) in order to protect other schools.

E-mail

- By default a School network user will have an e-mail address registered to their username
- When using this school e-mail address, users must behave in a manner that is appropriate to the ethos of the school
- Both incoming and outgoing e-mail is scanned for inappropriate terms, but the responsibility for the content of outgoing e-mail rests with the user
- The use of e-mail to bully, harass and intimidate others is forbidden. Where this is reported, it will be investigated and results passed to the appropriate authorities for disciplinary action
- Incoming e-mail containing attachments may be intercepted if either they appear to contain executable or command files. Where attachments are unusually large, stepped delivery times may be triggered

Webmail

As detailed in the SWGfL Filtering Policy, the School does not permit access to external e-mail services

Mobile Phones

- Student usage of mobile phones for voice and sms messaging is covered by the School's disciplinary Policy
- Any use of associated mobile phone technology (still and video cameras, sound recording devices) to capture non-consensual material and to distribute it to the detriment of students, staff or the School is forbidden.
- Staff usage of mobile phone technology is governed by existing legislation. In addition, staff should be aware of the published advice on staff e-safety.

Memory Devices

The use of USB memory pens/portable media players/external hard disks is permitted for the transfer of school-related files. Users are responsible for the

physical safety of such devices. All rules relating to the suitability of content on the School's network relate to such devices.

Laptops and PDAs

- Laptops and PDAs supplied by the School are treated as part of the School network and are bound by the same security and e-safety rules as outlined above
- Personal laptops and PDAs may not be connected to the School network
- The School reserves the right to confiscate and investigate the content and usage of any unnotified laptop or PDA found on the site

Social Networking

The School does not give access to external social networking sites. Where internal social networking takes place, in the form of weblogs and wickis, these will be set up by ICT Support staff and monitored by a named member of staff.

Images and Video

- On entry to the School, permission will be sought from the adult with parental responsibility to use electronic images of students for publicity or training purposes, using the School's Image Consent Form
- The School will store these images in the staff-only access area of the network for no longer than five-years unless additional permission is received from the adult with parental responsibility or from the child themselves if they have subsequently become adults
- Images without the appropriate consent or falling outside the five-year time limit will be deleted
- Adults with parental responsibility may request the removal of any image of their child, at any time
- To protect the identity of individuals, School will normally adopt the advice of South Gloucestershire Council that where a child's name is used, an image of them is not; where an image is used, the child's name is not
- Images taken for curricular purposes are the responsibility of the member of staff taking or authorising the taking of them. These images will be governed by the home-school agreement that each adult with parental responsibility will sign when their child is admitted to the School

School Website

- The School website exists to publish information about and to promote a positive image of the School
- All reasonable steps will be taken to protect the identity of students featured on the website
- The website manager is authorised to remove any content that contravenes any part of this Acceptable Usage Policy

SWGfL Portal and The Kingswood Partnership Extranet

- The School will provide user-information to allow staff and students to have accounts on both of these learning platforms
- Users are responsible for acquainting themselves the AUPs of these services

- Users must not assume that permissions granted on one platform are transferable to another

Reporting Abuse

- Students experiencing abuse or accidentally accessing inappropriate material should report it to a member of staff, immediately
- Staff experiencing abuse or accidentally accessing inappropriate material should report it to the ICT Support Department, immediately
- Procedures for reporting abuse arising from using the services of SWGfL are fully explained in their AUP. The e-mail address for reporting such matters is abuse@swgfl.org.uk

Sanctions

- There are instances of misuse that must be reported directly to the Police without any investigation by the School. These relate to the storage of child pornography or material that may contravene the Obscene Publications Act and where any investigation would involve the School itself in breaking the law by collecting evidence.
- Staff misuse will be dealt with using the agreed disciplinary procedures for staff
- It would be expected that sanctions against students would take into account that we are an educational institution and minor infringements followed by appropriate sanctions are part of the educational experience. More serious misuse will be dealt with using the students' disciplinary code.

5. Relationship to other Policies:

- Curriculum Policy
- Behaviours for Learning Policy

6. Monitoring, Review and Evaluation:

The monitoring of the implementation of this Policy will be the remit of:

- E-Safety Committee
- Curriculum Committee
- SLT

This Policy or sections of the Policy, may need reviewing and amending at any stage, due to the changing nature of technology and e-safety regulations.

Adopted by Full Governing Body on: 16.07.2008

Review Date: 2010