Montgomery High School

An Academy, Language College and Full Service School

Internet Policy

Linked Policies:

- Staff Code of Conduct
- Social Media Policy
- Anti-Bullying Policy
- Behaviour Policy
- Safeguarding and Child Protection

Approved by the Academic Standards Committee	24/10/12
Agreed review period	3 years

CONTENTS

APPENDICES

1. Aims

Protect students from internet-related dangers by providing students with as safe an internet environment as possible

Teach students about internet risk awareness and how to respond responsibly to the risks entailed

Enable the internet and emerging web-based technologies to be used and developed to advance learning

Support parents in gaining information relevant to securing safe internet access for students outside school

2. The Internet

Statement

The internet is an open communications channel, available to all. Applications such as the web, e-mail and chat all transmit information over the wires and fibres of the internet to many locations in the world. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the internet make it an invaluable resource used by millions of people every day.

Much of the material on the internet is published for an adult audience and some is unsuitable for students. In addition, there is information on weapons, crime and racism that would be more restricted elsewhere. E-mail and chat communication can provide opportunities for adults to make contact with children for inappropriate reasons.

3. Core Principles of Internet Safety

Statement

The internet is as commonplace as the telephone or TV and its effective use is an essential life-skill. Unmediated internet access brings with it the possibility of placing of students in embarrassing, inappropriate and even dangerous situations. Schools need a policy to help to ensure responsible use and the safety of students.

The Montgomery High School Internet Policy is built on the following five core principles:

Guided educational use

Significant educational benefits should result from curriculum internet use including access to information from around the world and the abilities to communicate widely and to publish easily. Curriculum internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful internet use will also reduce the opportunities for activities of dubious worth.

Risk assessment

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must learn to recognise and avoid these risks – to become “Internet Wise”.

Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and, students themselves taking responsibility for the use of internet and other communication technologies such as phones. The balance between educating students to take a responsible approach and the use of regulation and technical solutions must be judged carefully.

Regulation

The use of a finite resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within schools must simply be denied, for instance unmoderated chat rooms present immediate dangers and are banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help students make responsible decisions.

Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding students towards educational activities. Strategies must be suitable and their effectiveness monitored. There are no straightforward or totally effective solutions and staff, parents and everyone including students themselves must remain vigilant.

4. The Importance of Internet Use

Statement

- The purpose of internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

5. Potential Educational benefits of the Internet

Statement

- access to world-wide educational resources including museums and art galleries
- educational and cultural exchanges between students world-wide
- cultural, vocational, social and leisure use in libraries, clubs and at home
- access to experts in many fields for students and staff
- staff professional development through access to national developments, educational materials and good curriculum practice
- communication with support services, professional associations and colleagues
- improved access to technical support including remote management of networks
- exchange of curriculum and administration data
- mentoring of students and provision of peer support for students and teachers

6. Enhancement of Learning through the Internet

Statement

Increased computer numbers or improved internet access may be provided but effective use and quality of learning must also be addressed. Developing good practice in internet use as a tool for teaching and learning is clearly essential. Librarians, learning support assistants and teachers need to help students learn to distil the meaning from the mass of information provided by the web. Often the quantity of information needs to be cut down and staff could guide students to appropriate web sites, possibly by publishing lists for use at home. Offering students a few pre-approved sites will be more effective than suggesting they search the whole web!

Implementation:

- The school internet access will be designed expressly for student use and will include filtering.
- Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of students.
- Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

7. Evaluation of Internet Content

Statement

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop skills in selection and evaluation. Information received via the web, e-mail or text message requires good information handling skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read.

Ideally, inappropriate material would not be visible to students using the web but this is not easy to achieve and **cannot be guaranteed**. It is a sad fact that students may occasionally be confronted with inappropriate material, despite all attempts at filtering. Students should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening e.g. close the page and report the URL to the teacher or ICT Systems Manager for inclusion in the list of blocked sites.

More often, students will be judging reasonable material but need to select that which is relevant to their needs, for instance to answer a homework question. Students should be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Students should also use alternative sources of information for comparison purposes. Effective guided use should also reduce the opportunity students have for exploring unsavoury areas.

Access to sensitive sites, for example those that record the Holocaust, may be required for the duration of a specific educational activity by supervised students of appropriate age. Filtering software can provide temporary access to specific sites.

Using internet-derived materials in students' own work requires at least an understanding that straight copying is worth little without a commentary that demonstrates the selectivity used and evaluates significance. Respect for copyright and intellectual property rights, and the correct usage of published material should be taught.

Implementation:

- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Systems Manager.
- The school should ensure that the use of internet-derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
- Training should be available to staff in the evaluation of web materials and methods of developing students' critical attitudes.

8. E-mail

Statement

This aspect of The Montgomery High School Internet Policy augments the whole school internet/e-mail policy

E mail is an essential means of communication for both staff and students.

School e-mail should not be considered private and most schools, and indeed firms, reserve the right to monitor e-mail. There is a balance to be achieved between monitoring that is necessary to maintain the safety of students and the preservation of human rights, both of which are covered by recent legislation.

The use of personal e-mail addresses such as **john.smith@school.essex.sch.uk** needs to be carefully restricted to appropriate situations.

Many teenagers have their own e-mail accounts, such as the web-based Hotmail, which they use widely outside school. If e-mail accounts are not monitored there is the risk that students could send or receive inappropriate material. External web-based e-mail accounts with anonymous names such as **pjb354@emailhost.com** make monitoring difficult.

Much e-mail use is purely of a social nature and its impact upon learning needs to monitored and evaluated on an ongoing basis

Implementation:

- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Sending offensive e-mails is a serious matter and will be sanctioned in accordance with severity and the principles of the school behaviour policy
- Students must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

9. Web Site content

Statement

Web sites can celebrate students' work, promote the school and publish resources for projects or homework. Editorial guidance and quality control will ensure that the web site reflects the school's ethos and that information is accurate and well presented and that personal security is not compromised.

Our school's web site can be accessed by anyone on the Internet.

Publication of information must be considered from a security viewpoint.

Photographs that include students add a liveliness and interest to a web site that is difficult to achieve in any other way. Nevertheless, the security of staff and students must come first. Although common in newspapers, the publishing of students' names or class name with large photographs of students is not acceptable. Web images could be misused and individual students identified unless broad descriptions are used.

Strategies include using relatively small photographs of groups of students and using photographs that do not show faces at all. "Over the shoulder" can replace "passport-style" photographs but still convey the educational value of the activity.

With imagination it is possible to replace many personal photographs with self-portraits or images of students' work or of an activity such as a science investigation. A check should be made that students in photographs are appropriately clothed.

Photographs of a student must not be published without the parent's or carer's written permission.

Implementation:

- The point of contact on the web site should be the school address, school e-mail and telephone number. Staff or students' home information will not be published.
- Web site photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used on the web site in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school web site.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

10. Newsgroups and e-mail lists

Statement

Conferencing is a powerful method for students and teachers to share information and opinion. However, some conferencing applications, including chat and newsgroups can attract undesirable and irrelevant comment, often from anonymous elements.

Other collaboration tools such as moderated mailing lists and discussion facilities with a defined community of known users are far safer. Collaboration tools are covered in detail in the "Internet Users Guide" described in the reference section.

An e-mail distribution list can be the simplest method of distributing material to a set of selected users and is reasonably secure as the sender has complete control over who may join the list.

List servers automatically forward e-mail to a list of users. Lists can be private, where new users are added by the moderator or public, where anybody can join the list. A useful example is UK-schools: **www.jiscmail.ac.uk/lists/uk-schools.html**

A number of respected individuals or organisations including BECTa, LEAs and ICT suppliers run discussion groups. These can be an excellent way for the teacher with particular responsibility to share expertise with other staff over the UK, or indeed across the world. While the cost of hosting is low, the energy and organisation of the list or group moderator is essential to keep users on topic and ensure inappropriate postings do not occur.

Newsgroups or Usenet is a method of posting messages that can later be collected by any user interested in that particular topic. Some newsgroups are highly technical and others are dedicated to particular interests or hobbies. However, some are deeply disturbing. Open access to unmoderated newsgroups by contributors means that newsgroups can be infiltrated by the immature and offensive and for this reason, in general, should not be made available to students.

Access to the information in the best newsgroups can usually be obtained through list servers and e-mail lists.

Implementation:

- Newsgroups and e mail list facilities will not be made available to students unless an educational requirement for their use has been demonstrated.

11. Electronic 'Chat'

Statement

Chat is a popular conferencing application offering instantaneous exchange of text and images between groups of users via the Internet. In principle, chat has great potential for education; for instance students could exchange live text, speech or video with students in other countries. Such chat facilities would be moderated by the teacher and access would only be at times permitted by the teacher. Unauthorised persons would not know of the chat conference existence and therefore would not be able to gain access. Grid Club www.gridclub.com provides safe and interesting conferencing environments for students aged 7-11.

There are many varieties of chat including graphical chat areas using avatars (cartoons), instant messaging (IM) and chat hosted on web sites. Security varies widely and one has only to visit some chat rooms to be aware of the risks. Public, unregulated chat rooms can be used by the unscrupulous to gain access to children. Their use in school, even in a club setting, is highly debatable. Outside school, many students use a variety of chat facilities and may not be fully aware of the dangers.

Chat sites are banned by the school filtering system.

Implementation:

- Students will not be allowed access to public or unregulated chat rooms, or instant messaging services, unless specified by the school.
- A risk assessment will be carried out before students are allowed to use any new technology in school.

12. Emerging Internet applications including Social Networks

Statement

Many emerging communications technologies offer the potential to develop new teaching and learning tools. Mobile communications, wide internet access and multimedia present opportunities which need to be evaluated to assess risks, to establish benefits and to develop good practice. The safest approach is to deny access until a risk assessment has been completed and safety demonstrated.

Virtual classrooms and virtual communities can widen the geographical boundaries of learning. Students in two schools could complete a shared project using single class e-mail IDs and a web site. Staff and governors could make a larger community, which could be extended to include parents and commercial partners.

The safety of virtual communities depends on users being known and identifiable within the community. The registering of individuals to establish and maintain secure and validated electronic identities is an important and time-consuming part of the process.

Video conferencing introduces new dimensions. Cameras cost as little as £50 and, with faster internet access, enable limited video to be exchanged across the internet. The availability of live video can increase safety – you can see who you are talking to – but if inappropriately used, a video link could reveal security details.

New applications are continually being developed based on the internet, the mobile phone network and wireless or infrared connections. Users can be mobile using a phone or personal digital assistant with wireless internet access.

The inclusion of inappropriate language or graphical icons within text messages is difficult for staff to detect. Students may need reminding that such usage is both inappropriate and conflicts with school policy. Abusive text messages would come under the school anti-bullying policy.

Implementation:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during or between lessons unless as part of planned learning activity. The sending of abusive or inappropriate text messages is forbidden.

13. Authorising Internet access

Statement

The school will allocate internet access for staff and students on the basis of educational need. It will be clear who has internet access and who has not. Authorisation will be on an individual basis.

Parental permission will be required in all cases.

Implementation:

- The school will keep a record of all staff and students who are granted internet access. The record will be kept up-to-date, for instance a member of staff may leave or a student's access be withdrawn.
- Parents will be informed that students will be provided with supervised internet access (Appendix B).
- Students must apply for internet access individually by agreeing to abide by the Responsible Internet Use statement.

- For students under the age of 16, parents will be asked to sign and return an amalgamated internet use consent (Appendix C) and ICT Charter/Acceptable Use Protocol – System and Internet (Appendix D)
- For students above the age of 16 and not living at home or for students 18 or older, the school may rely on the consent of the student alone.

14. Assessing risk

Statement:

As the quantity and breadth of the information available through the internet continues to grow it is not possible to guard against every undesirable situation. .

Implementation:

The following disclaimers will be applied to student internet usage:

- In common with other media such as magazines, books and video, some material available via the internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher will ensure that the internet policy is implemented and compliance with the policy monitored.

15. Internet Filtering

Statement

Internet access must be appropriate for all members of the school community from youngest student to staff. Older secondary students, as part of a supervised project, might need to access adult materials; for instance a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily. Systems to adapt the access profile to suit the student's age and learning context are available.

The following technical strategies will be used to restrict access to inappropriate material (commonly described as filtering):

- **Blocking strategies** prevent access to a list of unsuitable sites or newsgroups.
- **A 'deny' list** preventing access to a list of non-approved sites.
- **Monitoring** records internet sites visited by individual user. Access to a site forbidden by the filtering policy will result in a report.

Filtering will take place both at school level and through an external provider (Internet Service Provider)

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content.

Careful monitoring and management of filtering systems is required.

Implementation:

- The school will work in partnership with parents, the LEA, DFE and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Systems Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal will be referred to the Internet Watch Foundation (please see references given later) and police will be informed.
- Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate.
- All incidents where unsuitable material breaches the school filtering system will be reported to the Headteacher and a log of such incidents will be maintained by the Director of the Technology College

16. Introduction of Internet Policy to Students

Statement

Many students are very familiar with internet use and culture. As students' perceptions of the risks will vary, the rules will need explanation and discussion. Students will need to be reminded of the school rules at the point of internet use. Consideration must be given to who should be teaching students safe practice and when and how this will be taught.

Implementation:

- Rules for internet access will be posted in all rooms where computers are used.
- Students will be informed that internet use will be monitored.
- Instruction in responsible and safe use should precede internet access.

17. Consultation

Statement

It is important that teachers and learning support assistants are confident to use the internet in their work. The School Internet Policy will only be effective if all staff subscribe to its values and methods. Staff will be given opportunities to discuss the issues and develop appropriate teaching strategies.

Staff must understand that the rules for any Montgomery High School employee on internet misuse are quite specific. Instances of misuse may result in dismissal. Any doubts as to the legitimacy of any aspect of their internet use in school, should be discussed with line managers to avoid any possible misunderstanding.

Implementation:

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any internet resource in school.
- All staff will be provided with the School Internet Policy, and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user and that discretion and professional conduct is essential.
- The monitoring of internet use is a sensitive matter. Staff who operate monitoring procedures will be supervised by senior management.

- Staff development in safe and responsible internet use and on the school internet policy will be provided as required.

18. Maintaining ICT System Security

Statement

It is important to review the security of the whole system, from user practice to Internet Service Provider (ISP).

Local Area Network (LAN):

- The user must act reasonably. Non-approved software must not be loaded. Good password practice is required including logout after use.
- The workstation should be secure from casual mistakes by the user.
- Cabling should be secure and wireless LANs safe from interception.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured to a high level.
- Virus and malware* protection for the whole network must be installed and current.

  **Malware or 'malicious software' is software designed to infiltrate a computer system, without a user's informed consent. The term is generally used to encompass all types of malicious software.*

Wide Area Network (WAN):

- All external connections must be assessed for security risks including the wide area network connection and any modems staff may wish to use.
- Firewalls and routers should be configured to prevent unauthorised use of software such as FTP and Telnet at the protocol level.

The internet is a connection to the outside world that could compromise system performance or threaten user or system security. The downloading of large files such as video and MP3 can compromise system performance. A wide area network (WAN) connection introduces further risks such as students trying to access another school. However it also brings the opportunity for industrial strength security in the form of hardware firewalls and the expertise to design and operate them.

Implementation:

- All students and (in addition) the parents of students under 16 years of age will be required to sign and return a copy of the Montgomery High School ICT Charter/Acceptable Use Protocol – Systems and Internet (Appendix D)
- The school ICT systems will be reviewed regularly with regard to security by the Systems Manager.
- Virus and malware protection will be installed and updated regularly by the Systems Manager and ICT technical support team.
- Security strategies will be discussed with our broadband provider.
- Personal data sent over the internet will be encrypted or otherwise secured.
- Use of portable media such as floppy disks, memory sticks and CD-ROMs by students is not allowed. Students wishing to carry data into school in such a fashion must pass the storage device to the Systems Manager for data transfer.
- Unapproved system utilities and executable files will not be allowed in students' file areas or to be distributed by any means e.g. e mail and will be deleted when found.

- Files held on the school's network will be regularly checked.
- The ICT Systems Manager will ensure that the system has the capacity to take increased traffic caused by internet use.

19. Complaints regarding Internet use

Statement

Where a complaint is received, the facts of the case will be established, for instance whether the internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline.

Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. Complaints of a child protection nature must be dealt with in accordance with Montgomery High School child protection procedures.

Implementation:

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Parents and students will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies.
- Sanctions available include:

  - interview/counselling by Progress Manager/Leader;

  - exclusion from school;

  - informing parents or carers;

  - removal of Internet and/or computer access for a period, which could ultimately prevent access to files held on the system.

20. Internet Use outside school

Statement

Internet use in students' homes is increasing rapidly, encouraged by offers of free access and continual media coverage. Unless parents are aware of the dangers, students may have unrestricted access to the internet.

Parents are advised to check if students' use elsewhere, such as libraries, is covered by an appropriate use policy.

Montgomery High School refers parents to web sites referred to in the references section of this document and advises that parents take the approach of keeping aware of developments and advising their children of the dangers.

The Childnet International site **www.chatdanger.com** has useful advice for students and parents.

Implementation:

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school web site.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged.
- Parents will be referred to organisations able to help

21. Internet use by our wider community

Statement

If the ICT facilities of the Montgomery High School are made available to members of our wider community for educational purposes, the safety and organisational principles outlined above will be retained in full.

Implementation:

Before access to the Montgomery High School ICT system:

- Adult community users will be required to sign the Montgomery High School Acceptable Internet Use and ICT Charter/Acceptable Use Protocol.
- Parents/carers of children under 16 years of age will be required to sign an acceptable use policy on behalf of the child.

22. Acknowledgements

This policy draws upon a model policy template produced by Kent County Council, whose copyright is hereby acknowledged

23. Monitoring

Governors will monitor implementation and review of the Montgomery High School Internet Policy through an ICT link Governor.

Implementation:

- Governors Academic Standards Committee will receive an annual report regarding internet safety, filtering and educational developments
- Serious internet safety breaches will be reported to the Governors' Student Welfare Committee without delay

24. Policy Revision

Internet technology and school use is changing rapidly, in addition Government guidance in areas such as e-mail, chat and websites continues to be revised.

This policy should be reviewed every 3 years

APPENDIX A

Montgomery High School

Responsible Internet Use

Rules for Staff and Students

The computer system is owned by the school. This Responsible Internet Use statement helps to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

- Irresponsible use may result in the loss of internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- School computer and internet use must be appropriate to the student's education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- The use of the internet to plagiarise work for submission for assessment is expressly forbidden
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
- Users are responsible for e-mail they send and for contacts made.
- Anonymous messages and chain letters are not permitted.
- The use of chat rooms and instant messaging services is not allowed, unless specifically approved.
- The school ICT systems may not be used for private purposes, unless the headteacher has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is not permitted.
- ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.
- Users who believe that their authorised account may have been compromised, for example by password credentials becoming insecure, must take immediate steps to protect their account by changing their password and/or informing the Systems Manager.

The school will exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

APPENDIX B

Montgomery High School

Acceptable Internet Use

Please complete, sign and return to the school office

Student: ***Form:***

Student’s Agreement

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and internet in a responsible way and obey these rules at all times.

Signed: ***Date:***

Parent’s Consent for Internet Access

I have read and understood the school rules for responsible internet use and give permission for my son / daughter to access the internet. I understand that the school will take all reasonable precautions to ensure students cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.

Signed: ***Date:***

Please print name:

Parent’s Consent for Web Publication of Work and Photographs

I agree that, if selected, my son/daughter’s work may be published on the school web site. I also agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not clearly identify individuals.

Signed: ***Date:***

APPENDIX C

Montgomery High School ICT Charter/Acceptable Use Protocol for the school ICT system and internet

The following are breaches of Montgomery High School's Network and Internet Protocol with consequences (in bold):

1. Allowing anybody to know your password for any reason.
2. Enabling anyone to access computer material, the network and/or Internet as a user other than themselves, whether they are banned or not, under your user name and password.
3. Attempting to access files or folders outside of my personal folder, student shared area or Clipart, or any other unauthorised material.
4. Using non-sanctioned communication, chat, or messenger services.
5. Accessing, non-sanctioned material unrelated to work during or beyond lessons.
   a. **Parents notified by letter**
   b. **Level 3 sanction, or higher**
   c. **Two week ban**

6. Gaining or attempting to gain access to the network and/or the Internet whilst banned.
   a. **Parents notified by letter**
   b. **Level 3 sanction, or higher**
   c. **A month ban**

7. Typing an unsuitable word into a search engine and/or typing an unsuitable URL (website address) into the address bar. ("Unsuitable" is defined as words/statements/material relating to computer based games (including consoles), material of a sexual nature, obscene/swear words, items relating to non-conformist groups or groups of questionable origin/beliefs/political views.)
8. Having, placing or attempting to place unsuitable material:
   - On any storage medium
   - In your user folder on the network
   - In a shared network area
   - On a laptop/palmtop or other electronic device
9. Pursuing or attempting to pursue unsuitable results from a search of the above type. Viewing or attempting to view or download any unsuitable results.
10. Entering/attempting to enter a site despite filtering warnings about unsuitable content.
11. Attempting to by-pass. circumvent internet filters by any means
12. Downloading or attempting to download any unsuitable material in any electronic format.
13. Sending or attempting to send any unsuitable material using any type of email.
    a. **Parents notified by telephone and letter**
    b. **After an appropriate investigation by a member of the Senior Leadership Team, potential external exclusion of at least one day**
    c. **Unlimited (but time defined) ban**

NOTE: Material and/or actions suspected of illegality will be referred to the police and Internet Watch Foundation. A Deputy Headteacher may suspend any ban to allow planned curriculum activity.

PARENT/CARER: I have read and understand the AUP. I acknowledge that the college will take every step possible to ensure that unsuitable content is not accessible to my son/daughter/ward whilst using a computer in school. I also accept that the responsibility to adhere to the policy is that of my son/daughter/ward and a breach of any of the conditions above will lead to the indicated sanction being imposed on them. I hereby give my son/daughter/ward permission to use the school computer network facilities, including the Internet.

Parent/guardian signature .... Print Name ....

STUDENT: I have read and understand the AUP. I know that the school will take all steps available so that I cannot access unsuitable content whilst I am using a computer in school. It is my responsibility to exercise common sense and caution when using the computers in school. It is my responsibility to abide by the AUP above and I understand that if I do break the rules I will be subject to sanctions. I understand that I may only use the school computers for school work. I understand that I am fully responsible for the security and content of my own user area and school e mail account and must report any suspected loss of security to the Systems Manager immediately.

Student signature .... Print name ....

Please sign both copies. Keep one copy safe for future reference and return the second copy to school in the envelope provided.

APPENDIX D

References

CEOP – Child Exploitation and Online Protection Centre **http://www.ceop.gov.uk**

Know IT All For Parents http://www.childnet-int.org/kia/parents/

Byron Review – Children and new Technology **http://www.dcsf.gov.uk/byronreview/**

Bullying Online **www.bullying.co.uk**
Advice for children, parents and schools

Kidsmart **www.kidsmart.org.uk**
An Internet safety site from Childnet, with low-cost leaflets for parents.

Think U Know? **www.thinkuknow.co.uk/**
Home Office site for students and parents explaining Internet dangers and how to stay in control.

Family Guide Book (Government recommended **www.familyguidebook.com**
Information for parents, teachers and students

Action for Children www.**actionforchildren**.org.uk
Expert advice for children, young people and parents.

Safekids **www.safekids.com**
Family guide to making Internet safe, fun and productive

NAACE / BCS **www.naace.org** (publications section)
A guide for schools prepared by the BCS Schools Committee and the National Association of Advisers for Computer Education (NAACE)

Internet Watch Foundation - **www.iwf.org.uk**
Invites users to report illegal Web sites

Data Protection **www.ico.gov.uk**
Information Commissioner

Kent Web Skills Project **www.kented.org.uk/ngfl/webskills/**
Discussion of the research process and how the Web is best used in projects.

Click Thinking: Scottish Education Department **www.scotland.gov.uk/clickthinking**
Comprehensive safety advice

DotSafe – European Internet Safety Project **http://dotsafe.eun.org/**
A comprehensive site with a wide range of ideas and resources, some based on Kent work.

APPENDIX E

Notes on the legal framework

This page must not be taken as advice on legal issues, rather as non-specialist guidance.

The Computer Misuse Act 1990 makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day to day activities.

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

The Rules for Responsible Internet Use, which every user must agree to, contain a paragraph that should ensure users are aware that the school is monitoring internet use.

In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring.

The following legislation is also relevant:

Data Protection Act 1984/98 concerns date on individual people held on computer files and its use and protection.

Copyright, Design and Patents Act 1988 makes it an offence to use unlicensed software

The Telecommunications Act 1984 Section 43 makes it an offence to send offensive or indecent materials over the public telecommunications system.

Protection of Children Act 1978

Obscene Publications Act 1959 and 1964 defines "obscene" and related offences.

References:

Brief introduction to dangers and legal aspects of the internet.

www.bbc.co.uk/webwise/basics/user_01.shtml

List of useful law resources; see copyright and internet sections.

http://link.bubl.ac.uk/law

HMSO: Full text of all UK legislation and purchase of paper copies.

www.legislation.hmso.gov.uk