



Inspiring Learners for their future

E-SAFETY POLICY

UPDATED FEBRUARY 2011

Consultation History

Governors/staff/parents/students	Date
Executive (Leadership Group)	
Teaching and Non-Teaching Staff	
Curriculum Committee	
Full Governing Body	February 2011
Next Review of Policy	

E-Safety Policy 2011

Contents

Definition	5
1. Background	6
2. Teaching and Learning	7
2.1 Managing information Systems	9
2.2 Policy Decisions	16
2.3 Implementation Policy	18
Appendix 1 - Student Acceptable Use	20
Appendix 2 - Staff Acceptable Use	23
Appendix 3 - Parent Acceptable Use	26
Appendix 4 - Legislation relating to technologies	28



The Ridgeway School & Sixth Form College

E - Safety Policy 2011

Definitions

Staff

Any person who is employed by The Ridgeway School & Sixth Form College.

Student

Any person is studying at The Ridgeway School & Sixth Form College.

Parent

A person who has a parental responsibility for at least one student who is studying at The Ridgeway School & Sixth Form College.

Trainee Teacher

Any person who is training to become a qualified teacher. Where a Trainee Teacher is also employed by the school in the case of a GTP then they will be considered staff in this policy.

Volunteer

Anyone who is helping within the school unpaid.

School Network

Any device that is connected to the school network.

Learning Platform

The school learning platform FROG (<http://frog.ridgeway.swindon.sch.uk>) that is used by staff, students and parents to enhance the learning of students.

1.0 Background / Rationale

The school e-safety policy helps to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the student themselves. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with the Behaviour for Learning Policy, the Anti-bullying and the Safeguarding policy (child protection)

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

1.1 Development / Monitoring / Review

The e-Safety Policy is part of the ICT and Safeguarding Policies. It also relates to other policies including those for behaviour, anti-bullying, personal, social and health education (PSHE) and for citizenship.

This E-safety policy has been developed by the E-safety committee made up of –

Deputy Headteacher,	J. Povoas
E Learning co-ordinator,	G. Mitchell
Head of ICT,	D. Scott
AHT Safeguarding and Student Support,	J. White
Link Governor for E-Safety,	J. Crowley
IT Support Manager,	
Parents and carers,	Parent Council
Frog Prefects,	Students

2.0 Teaching and Learning

2.0.1 Importance of Internet Use

The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through ICT and Internet use.

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The Internet is a part of everyday 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.
- Students use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- 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 functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

2.0.2 Educational Benefits

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased student attainment.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between students worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with SBC and DCSF;
- access to learning wherever and whenever convenient.

2.0.3 Enhance Learning

Increased computer numbers and improved Internet access may be provided but its impact on students learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Students need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material will be taught across the curriculum. Methods to detect plagiarism may need to be developed.

- The school's Internet access will be designed to enhance and extend education.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and students complies with copyright law.
 - Access levels will be reviewed to reflect the curriculum requirements and age of students.
 - Staff should guide students to online 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.
 - Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

2.0.4 Evaluation of Internet Content

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach will be taken.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc provide an opportunity for students to develop skills in evaluating Internet content. For example researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching/learning in every subject.

2.1 Managing Information Systems

2.1.1 Information Security

Network Manager Responsibilities

- Workstations will be secured against user mistakes and deliberate actions.
- Servers will be located securely and physical access restricted to authorised persons.
- The server operating system will be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed.
- Decisions on WAN security are made on a partnership basis between The Ridgeway School & Sixth Form College and SWGfL.

Staff, Student and Parent Responsibilities

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. *See Appendix 1.1, 1.2, 2 and 3 for AUPs*
- Personal data sent over the Internet or taken off site will be encrypted, except where this data is limited to a teacher's mark book and contains no more than names and grades.
- Unapproved software will not be allowed in students' work areas or attached to email.
- Files held on the school's network will be regularly checked.

e-Safety Committee

- The e-safety committee will review IT security as part of its monitoring on a tri-yearly basis.

2.1.2 School Password Policy

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E-Safety Committee.

The following rules apply to the use of passwords for staff and students

- passwords must be changed three times per year
- the last four passwords cannot be re-used
- the password should be a minimum of 8 characters long and
- must include three of – uppercase character, lowercase character, number, special character
- the account should be “locked out” following six successive incorrect log-on attempts

- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on

The “administrator” passwords for the school ICT system, used by the IT Support Manager must also be available to the Headteacher and kept in a school safe. The school will never allow one user to have sole administrator access.

2.1.3 School IT Security

The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another’s files, without permission (or as allowed for monitoring purposes within the e-safety policy).
- access to personal data is securely controlled in line with the school’s personal data policy
- logs are maintained of access by users and of their actions while users of the system
- Due to the sensitive nature of data stored on SIMs Trainee Teachers will not be provided with their own SIMs access. It is expected that Trainee Teachers will use SIMs under supervision of the teacher who has responsibility for the class being taught.

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email and the Virtual Learning Environment (VLE).

Responsibilities

- The management of the password security policy will be the responsibility of IT Support Manager
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- Passwords for new users and replacement passwords for existing users can be allocated by IT Support. Any changes carried out must be notified to the manager of the password security policy (above).
- Users will change their passwords three times per year.

Training / Awareness

Members of staff will be made aware of the school’s password policy:

- At induction
- Through the AUP

Student will be made aware of the school’s password policy:

- In ICT Lessons
- Through the AUP

2.1.4 E-Mail Management

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

In the school context (as in the business world), email should not be considered private and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of students and the preservation of human rights, both of which are covered by recent legislation.

Spam, phishing and virus attachments can make email dangerous. The SWGfL uses industry leading email relays to stop unsuitable mail using reputation filtering, currently about 95% of mail is rejected as spurious.

- E-Mail for all users is limited to approved school e-mail (Outlook / Frog). Access to personal e-mail is blocked by school filters
- Student e-mail at KS3 / KS4 is limited to Internal e-mails¹
- Staff and Sixth Formers will be provided with an Outlook e-mail account in addition to a Frog e-mail account allowing the sending of e-mails externally.
- All e-mails are logged and e-mails sent through the school learning platform can be recalled.
- Students must immediately tell a teacher if they receive offensive email.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
 - Excessive social email use can interfere with learning and will be restricted.
 - The forwarding of chain messages is not permitted.
 - Staff should only use school email accounts to communicate with Students in a professional dialog
 - **Staff should not use personal email accounts for professional purposes**
- **Trainee Teachers will not be added to any staff distribution lists.**

2.1.5 Published Content – School Website

The school's official website www.ridgewayschool.com is used as a publicity and communication channel with stakeholders.

Sensitive information about schools and students could be found in a newsletter but a school's website is more widely available. Publication of information should be considered from a personal and school security viewpoint.

- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- Images and student names will not be published on the school website.
- Students in photographs will be appropriately clothed.
- Images of students will be of limited quality reducing the risk of the image being taken and used elsewhere on the Internet.
- Parents or carers will have the opportunity to opt out of having images of their child or their child's work published.

¹ Internal refers to e-mails existing on the school learning platform Frog. These e-mails can be accessed internationally although e-mails cannot leave the learning platform.

2.1.6 External Collaborative Websites

Where it is impossible for a school to provide an internal system that provides students with the same learning benefits as an external system this can be authorised by the Headteacher and recorded in a log held by the e-learning co-ordinator. Provided the following criteria are met:

- The site is secured so that only students from The Ridgeway School & Sixth Form College can collaborate together or where students can communicate with other users of the site it can be reasonably be expected that these other users meet the same safeguarding standards as workers at the school.
- It is important to note how a free tool could be funded and to be aware of advertising, especially as adverts seen from outside school may not be subject to the same filtering system as used in school.
- The site must only be used for professional communications.
- An administrator password must be provided and logged in the e-safety policy.

2.1.7 Internet Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a part of the South West Grid for Learning (SWGfL) schools and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Changes to the filtering system

The responsibility for the management of the school's filtering policy will be held by the Network Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the SWGfL / school filtering service must:

- be logged in a change control log
- be reported to the E-Safety Co-ordinator every week
- where a change is questionable about the educational benefit the request will be forwarded to the Headteacher who will have the final decision.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the E-Learning Co-ordinator / Network Manager who will decide whether to make school level changes (as above). If it is felt that the site should be filtered (or unfiltered) at SWGfL level, the responsible person E-Learning Co-ordinator / Network Manager should email filtering@swgfl.org.uk with the URL.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Staff

Should an inappropriate site be accidentally accessed in school or out of school this must be immediately reported to the Network Manager or E-Learning Co-ordinator. A log of incidents will be held and taken to the e-safety committee meetings.

Staff will be made aware of the filtering system through:

- Signing the AUP
- Induction training
- Staff meetings, briefings and insets

Students

Students will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Parents

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions / newsletter etc.

2.1.8 Unfiltered Internet

Staff will be able to apply for Unfiltered Internet to the Staff Proxy. It is vitally important that staff are aware that when using the Internet with such access filtering is only limited to the IWF list². The result of this is that inappropriate content could very easily be shown on screen. Staff should be aware of dynamic webpages which may have changed from when the content was last checked.

- Staff using unfiltered Internet are still monitored as they would be on the filtered connection.
- Staff must never leave a machine where students could access unfiltered Internet.
- It is not recommended to do live searches on the Internet in front of a class when you are signed into the Staff Proxy and receiving unfiltered internet.
- The use of unfiltered Internet should only be used to access content that benefits teaching and learning and in these cases it should be assessed against the safeguarding risks of using an unfiltered resource.
- In case of inappropriate content being shown the computer should be disconnected from all screens immediately and logged to IT Support.

2.1.9 Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use agreement.

² The IWF list is a dynamic filter used by many ISPs that blocks child sexual abuse images.

2.1.10 Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- Headteacher / Senior Leadership Team
- E-Learning Co-ordinator
- E-Safety Committee
- E-Safety Governor / Governors committee
- SWGfL / Local Authority on request
- Staff should report any accidental access to inappropriate content to IT Support (wherever this may occur on a school device). This will allow IT Support to decide if any clearing of browser history etc is required to prevent any students from being exposed to content. Details of incidents will be logged and reviewed as part of the e-safety committee meetings.

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision

2.1.11 How can emerging technologies be managed?

Emerging technologies will be discussed by the e-safety committee and approval of future systems will be on the basis of a risk assessment taking into account risk vs. benefits to education.

2.1.12 Protection of Personal Data

The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

The Ridgeway School & Sixth Form College already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

Information Commissioner's Office: <http://www.ico.gov.uk/>

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.2 Policy Decisions

2.2.1 Authorising Internet Access

The school will allocate Internet access for staff and students on the basis of educational need. Authorisation is on an individual basis. Parental permission will be required for Internet access in all cases — this will be checked annually when students' home details are checked and as new students join.

- The school will maintain a current record of all staff and students who are granted access to the school's network.
- All staff must read and sign the 'Staff AUP' before using any school ICT resource.
- Students must apply for Internet access individually by agreeing to comply with the e-Safety Rules.
- Parents will be asked to sign and return a consent form for student access.

2.2.2 Risk Assessments

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will inform parents and students that it is not possible to completely remove the risk that students might access unsuitable materials via the school system. This is beneficial as it allows the teaching of responsible internet use where students may have access to unfiltered internet outside of school or via personal devices.

- The school will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate.
 - 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.

2.2.3 Complaints Procedure

Complaints will be handled in line with the schools complaints procedure.

2.2.4 Cyberbullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

Many young people and adults find using the internet and mobile phones a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.

- Cyberbullying education will form part of students' e-safety lessons
- There will be clear procedures in place to support anyone affected by Cyberbullying.
 - All incidents of cyberbullying reported to the school will be recorded in line with the school Anti Bullying Policy.
 - The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying may include (in addition to the school Anti Bullying policy):
 - The bully will be asked to remove any material deemed to be inappropriate or offensive.
 - A service provider may be contacted to remove content.
 - Internet access may be suspended at school for the user for a period of time.
 - Parent/carers may be informed.
 - The Police will be contacted if a criminal offence is suspected.

2.2.5 Management of the School Learning Platform (Frog)

The Learning Platform/Environment is subject to careful monitoring by the E-Learning Co-ordinator / Senior Leadership Team (SLT). The E-Learning Co-ordinator has a duty to review and update the policy regarding the use of the Learning Platform annually and all users must be informed of any changes made.

- SLT and staff will monitor the usage of the Learning Platform by students, parents and staff regularly in all areas, in particular message and communication tools and publishing facilities.
- Students/staff will be advised on acceptable conduct and use when using the learning platform.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, students (and associated parents) etc leave the school their account or rights to the LP will be disabled
- Any concerns with content may be recorded and dealt with by Appendix 1.2 Student Sanctions.
- A visitor may be invited onto the LP by a member of the SLT / E-Learning Co-ordinator. In this instance there may be an agreed focus or a limited time slot.
- Parents will accept the Parent AUP at every logon to the Learning Platform –see *appendix 3*.

2.3 Implementation Policy

2.3.1 Student Education

Students will follow a discrete ThinkuKnow SoW at the beginning of each year in KS3 and a refresher lesson each year in KS4.

Additionally:

- All users will be informed that network and Internet use will be monitored.
- Student instruction in responsible and safe use should precede Internet access.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where students are considered to be vulnerable.

2.3.2 Staff Education

It is important that all staff feel confident to use new technologies in teaching and the School e–Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies.

All staff will be told the rules for information systems misuse for employees are specific and instances resulting in disciplinary procedures and dismissal have occurred. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

Staff will be informed about the safe and appropriate use of school provided equipment and rules outside of school Staff who have been issued with a laptop must not allow any non-employee of The Ridgeway School & Sixth Form College to use the laptop. Staff must be made aware of their responsibility to maintain confidentiality of school information.

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and students, the school will implement Acceptable Use Policies.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user, Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.

2.3.3 Parent Education

Internet use in students' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, students may have unrestricted and unsupervised access to the Internet in the home. The school will help parents plan appropriate supervised use of the Internet at home and educate them on the risks. Parents should also be advised to check if their child's use elsewhere in the community is covered by an appropriate use policy. One strategy is to help parents to understand more about ICT — perhaps by running courses and parent awareness sessions, although the resource implications will need to be considered.

- Parents’ attention will be drawn to the School e–Safety Policy in newsletters, the school brochure and on the school website.
- Parents will be requested to sign an e–Safety/internet agreement as part of the Home School Agreement.
- Information and guidance for parents on e–Safety will be made available to parents in a variety of formats, including on the school learning platform.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents through the school learning platform.
- Interested parents will be referred to organisations listed in section “e–Safety Contacts and References.”

e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre):

<http://www.ceop.police.uk>

Childline:

<http://www.childline.org.uk>

Childnet:

<http://www.childnet.com>

Children’s Safeguards Service:

<http://www.swindonlscb.org.uk>

Click Clever Click Safe Campaign:

<http://clickcleverclicksafe.direct.gov.uk>

Cybermentors:

<http://www.cybermentors.org.uk>

Digizen:

<http://www.digizen.org.uk>

Internet Watch Foundation:

<http://www.iwf.org.uk>

Kidsmart:

<http://www.kidsmart.org.uk>

SWGfL:

<http://www.swgfl.org.uk/staying-safe>

Teach Today:

<http://en.teachtoday.eu>

Think U Know website:

<http://www.thinkuknow.co.uk>

Virtual Global Taskforce — Report Abuse:

<http://www.virtualglobaltaskforce.com>

Swindon Borough Council – Local Safeguarding Board

<http://www.swindon.gov.uk/lscb-index/lscb-families-home/lscb-families-internet.htm>

Appendix 1.1 – Student Acceptable Use of Policy

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network/ learning platform, FROG SERVER, with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone.
- I will only use my school e-mail address.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will switch my screen off and report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the Head Teacher, Mr Colledge.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

Appendix 1.2 – Student Sanctions

Sanctions for breaking the schools acceptable ICT use policy

In ICT lessons offences should be referred to the Head of ICT in other subject areas the e-learning co-ordinator.

C1 (equivalent to W1)

- Food and drink
- Off task behaviours e.g. websites, games, etc
- Downloading without permission
- Inappropriate/excessive printing
- Inappropriate use of external devices e.g. USB, mp3, mp4, mobile phones etc.

Sanction

- As W1.

C2 (equivalent to W2)

- Repeated C1 offences
- Disconnecting cables, devices etc or changing settings
- Minor damage to equipment
- Abusing others work
- Logging on as another student and/or sharing passwords
- Inappropriate use of internet, including accessing sites that you have not been directed to use
- Inappropriate use / storage of text, images, sound, video and other media
- Inappropriate use of approved collaboration tools; such as school e-mail and Frog social networking
- Failure to report accidental access to inappropriate content

Sanction

- Break time detention issued
- Letter home detailing unacceptable use
- Charge for any damage caused
- Learning Platform Social Networking tools disabled for 1 week.

C3 (equivalent to W3)

- Repeated C2 offences
- The sending of communications that could be regarded as offensive³, harassing or bullying in nature through any of: school learning platform or school network.
- Damage to equipment
- Attempting to access any sites of a pornographic nature
- Storage of any images of a pornographic nature
- Logging onto the system using a non-student account (staff, parent etc)
- Corrupting work of another user

Sanction

³ Offensive – Any communication that causes a reasonable adult to feel resentful, upset or annoyed by.

- Pastoral after school detention issued
- Letter home detailing unacceptable use
- Charge for any damage caused
- Possible Internet ban – any ban agreed with Deputy Head, Head of ICT and E-Learning Co-ordinator.
- Learning platform social networking tools disabled for 4 weeks

C4 – Referral to Deputy Head

- Hacking
- Bypassing security settings
- Using proxy sites
- Major damage to equipment
- Cyber bullying (referral to J White in first instance)
- Unauthorised access
- Any offence which is directly detrimental to a large group (over 30) of students learning.
- Any offence which could bring the school into disrepute

Sanction

- Internal / External Exclusion

Illegal Activities

- Illegal activity: this will be dealt with by the Headteacher / Deputy Headteacher and external agencies in line with the SWGfL policy and the law.

Appendix 2 – Staff Acceptable Use Policy

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *student* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that student receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- **I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.**
- ***I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Network Manager, E-Learning Co-ordinator or Head Teacher.***

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- **I will only communicate with student and parents / carers using official school systems. Any such communication will be professional in tone and manner.**
- **I will not engage in any on-line activity that may compromise my professional responsibilities.**

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission from the Network Manager) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- **I will immediately report any damage or faults involving equipment or software to IT Support, however this may have happened.**

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- **I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority, dismissal and in the event of illegal activities the involvement of the police.**

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Signed: _____

Date: _____

Staff / Volunteer
Name: _____

Appendix 3 – Parent / Carer Acceptable Use Policy

Introduction

The Frog Server is hosted on the school site and all communications to and from the frog server travels via the SWGfL who provide the school's broadband connection. Anything detailed here is in addition to and does not replace anything laid out in the SWGfL AUP. It is important to note that SWGfL proactively monitor communications on their network for any illegal activities and will notify appropriate authorities where necessary.

Legal

The Computer Misuse Act 1990 applies to the use of any computer system including the Frog server. If you carry out any of the following actions you may be committing a criminal offence.

Unauthorised access to computer materials

Unauthorised access with intent to commit or facilitate commission of further offences

Unauthorised modification of computer material

Account Security

- You are responsible for the security and use of your Username and Password.
- You are not allowed to use the account, Username or Password of any other user.
- You must not disclose your Username or Password to anyone else.

If you think that your account has been compromised you must contact the school as soon as possible to reset your password.

Communication

When using the communication facilities (forums) YOU MUST:

- Respect other people's views and beliefs.
- Only post comments which are appropriate to the particular discussion.
- Remember that you are conversing with real people.
- By contributing posts to any forum within the parent portal you are granting a license to the school to reproduce the content of your posting, and you are also granting a license to other users to download or copy the content in accordance with these conditions.
- You must give due acknowledgement for material quoted from other sources.

When using the communication facilities YOU MUST NOT:

- Post anything abusive, defamatory, obscene or otherwise illegal.
- Post any personal or private information on any individual.
- Use forums to air grievances, grievances should be made in accordance with school procedures.
- Copy or forward any communication without permission.
- Include material which is confidential or the copyright of which is owned by someone else, unless you have first obtained permission.
- Post material which contains viruses or other programs which may disrupt the school's systems.
- Post any advertising or promotional material.
- Behave in an impolite or offensive manner.

Copyright

You are permitted to view, copy, and print documents hosted within the parent portal subject to your agreement that:

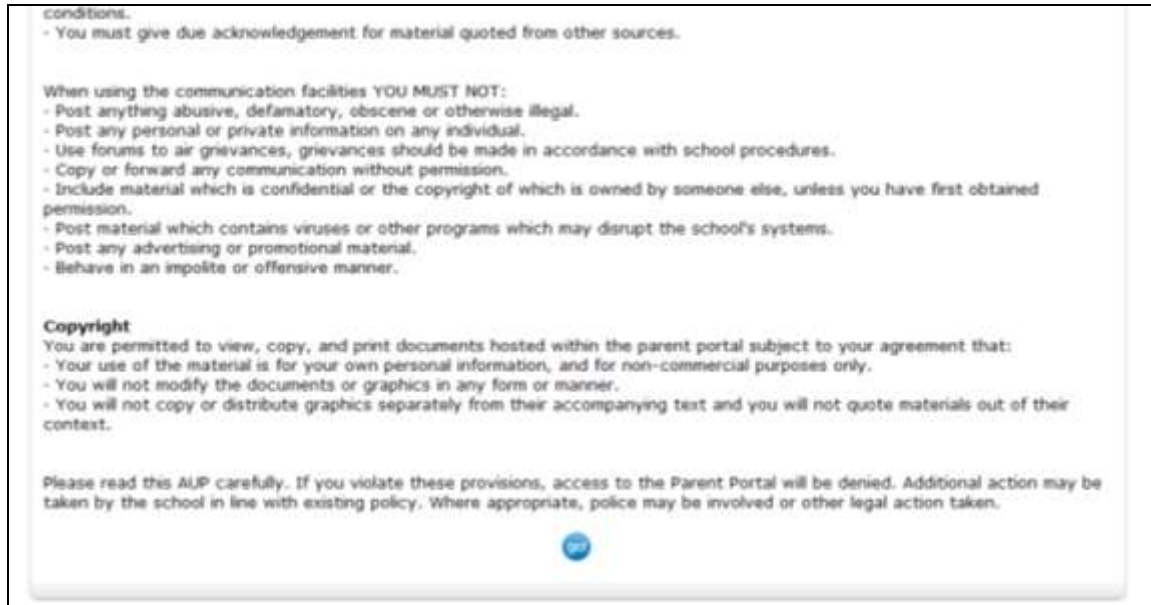
- Your use of the material is for your own personal information, and for non-commercial

purposes only.

- You will not modify the documents or graphics in any form or manner.
- You will not copy or distribute graphics separately from their accompanying text and you will not quote materials out of their context.

Please read this document carefully. If you violate these provisions, access to the parent portal will be denied. Additional action may be taken by the school in line with existing policy. Where appropriate, police may be involved or other legal action taken.

Parents agree to this AUP on every logon to the learning platform as shown below:



Appendix 4 – Legislation Relating to Technologies

The user must comply with all relevant legislation and legal precedent, including the provisions of the following Acts of Parliament, or any re-enactment thereof:

[Copyright, Designs and Patents Act 1988](#);

[Malicious Communications Act 1988](#);

[Computer Misuse Act 1990](#);

[Criminal Justice and Public Order Act 1994](#);

[Trade Marks Act 1994](#)

[Data Protection Act 1998](#);

[Human Rights Act 1998](#);

[Regulation of Investigatory Powers Act 2000](#);

[Freedom of Information Act 2000](#);

[Communications Act 2003](#).

See below for a summary of the main points.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Computer Misuse Act 1990

This Act makes it an offence to:

Erase or amend data or programs without authority;

Obtain unauthorised access to a computer;

"Eavesdrop" on a computer;

Make unauthorised use of computer time or facilities;

Maliciously corrupt or erase data or programs;

Deny access to authorised users.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

The right to a fair trial

The right to respect for private and family life, home and correspondence

Freedom of thought, conscience and religion

Freedom of expression

Freedom of assembly

Prohibition of discrimination

The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

Establish the facts;

Ascertain compliance with regulatory or self-regulatory practices or procedures;

Demonstrate standards, which are or ought to be achieved by persons using the system;

Investigate or detect unauthorised use of the communications system;

Prevent or detect crime or in the interests of national security;

Ensure the effective operation of the system.

Monitoring but not recording is also permissible in order to:

Ascertain whether the communication is business or personal;

Protect or support help line staff.

The school reserves the right to monitor its systems and communications in line with its rights under this act.