Rowlands Gill Primary School

ICT Policy

Date: July 2015

Ratified by Governors: July 2015

Review Date: November 2017

Category: Safeguarding
Authorised By: Full Governing Body
Author Headteacher – Miss Martin & Computing Subject Leader – Mrs Readshaw
Designated person for CP – Miss Martin
Designated person for E- safety -
Version: 1

Issue Date: July 2015
Next Review Date: NOV 2017 & checked annually for relevance

We are a Rights Respecting School:

Article 3: Everyone who works with children should always do what is best for each child.

Article 13: Your right to have information.

Article 16: Your right to privacy.

Article 19: You should not be harmed and should be looked after and kept safe.

Article 36: You should be protected from doing things that could harm you.

Rowlands Gill Primary - E-Safety and Acceptable Use Policy

E-Safety encompasses internet technologies and electronic communications such as mobile phones, iPads and wireless technology. Most young people are enthusiastic Internet users - particularly of interactive services like: Email, Chat and Instant Messaging. However, like many exciting activities, there are risky situations to deal with and hazards to avoid. Robust policies and procedures, clear roles and responsibilities, a comprehensive safety education programme for pupils, staff and parents and an effective range of technological tools to support e-safety are essential to providing a safe ICT learning environment.

Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using technology, media and information resources, is one that the school shares with parents and carers. At the Rowlands Gill Primary School, we feel that the most successful approach lies in a combination of site filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

Context

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.
To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- E-mail
- Instant messaging / video messaging (e.g. Skype) using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Smart phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications. Tablets and iPads.

The 2014 National Curriculum
Taken from: Computing in the National Curriculum. A guide for Primary School Teachers. Published by CAS and written in collaboration by CAS and Naace members, Published 2013. Author: Miles Berry

Computers are now part of everyday life. For most of us, technology is essential to our lives, at home and at work. 'Computational thinking' is a skill children must be taught if they are to be ready for the workplace and able to participate effectively in this digital world. The new national curriculum for computing has been developed to equip young people in England with the foundational skills, knowledge and understanding of computing they will need for the rest of their lives. Through the new programme of study for computing, they will learn how computers and computer systems work, they will design and build programs, develop their ideas using technology and create a range of content.

Computing is concerned with how computers and computer systems work, and how they are designed and programmed. Children studying computing will gain an understanding of computational systems of all kinds, whether or not they include computers. Computational thinking provides insights into many areas of the curriculum, and influences work at the cutting edge of a wide range of disciplines. Why is computational thinking so important? It allows us to solve problems, design systems, and understand the power and limits of human and machine intelligence. It is a skill that empowers, and one that all children should be aware of and develop competence in. Children who can think computationally are better

able to conceptualise, understand and use computer-based technology, and so are better prepared for today's world and the future.

Across the curriculum, children learn to:

- Find and select information from digital and online sources, making judgments about accuracy and reliability.
- Create, manipulate and process information using technology to capture and organise data, in order to investigate patterns and trends; explore options using models and simulations; and combine still and moving images, sounds and text to create multimedia products.
- Collaborate, communicate and share information using connectivity to work with, and present to, people and audiences within and beyond the school.
- Refine and improve their work, making full use of the nature and pliability of digital information to explore options and improve outcomes.

Policies and Procedures

- The school's e-safety policy will operate in conjunction with other policies including: **Behaviour, Anti-Bullying, Teaching and Learning and Data Protection. It will also be linked with our Rights Respecting Schools Award.**
- It has been approved by governors.
- The E-safety Policy and its implementation will be reviewed annually and where necessary in cases of reported misconduct or risks.
- All Rowlands Gill, staff, parents and pupils are asked to sign an Acceptable Use Policy/leaflet (AUP) detailing the ways staff, parents, pupils and all network users should use our ICT facilities and reflects the need to raise awareness of the safety issues associated with electronic communications as a whole. The AUP will be displayed in all classrooms.
- E -safety will form a key part of the Computing/PSHE curriculum. Children will be made aware of the dangers and risks of using the internet and mobile technologies throughout the school year. This will include learning about issues during RRSA weeks, Anti-Bullying/Safe School Week and will form an integral part of ICT lessons.

All staff (including teachers, admin staff, supply staff and classroom assistants) and any other adults involved in supervising children accessing the Internet, will be provided with E Safety and Acceptable Use Policy, and will have its importance explained to them. Parents' attention will be drawn to the policy by letter in the first instance and, thereafter, in our school brochure and on the school's website. The policy is available for parents and others to read on the school website and on demand.

We have a major responsibility to educate our pupils, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies.

Yet at the same time we recognise that the use of these new technologies can put young people at risk within and outside the school.

The most serious risk to children using the internet involves the possibility of someone being hurt, exploited or abused as a result of personal information being disclosed online. Pictures, names, addresses, ages or information about a child's likes or dislikes can be used to trace, contact and meet a pupil with the intention of causing harm.

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.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. E Safety issues can also affect adults who work or are associated with the school. For example school and personal data being entered on web/social networking sites, fraudulent email traps and cyberbullying. It is impossible to eliminate risk completely. It is therefore essential, through good educational provision to manage the risk and deal with any threat to safety.

The school will take all reasonable precautions to ensure E Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Internet Access

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school's Internet access is designed expressly for pupil use and uses the **Omnicom Service** and filtering system.

- Pupils are taught what Internet use is acceptable and what is not and are given clear objectives for Internet use. Pupils will not use the internet without having permission and **MUST be supervised at all times from a member of staff.**

All staff are aware that a filtering system can reduce but cannot eliminate the risk of exposure to inappropriate material on the Internet. <u>This is why no child must be allowed to access the Internet without adult supervision</u>.

Staff laptops and devices MUST be locked when not in use. (They should not be left unattended in the classroom.)

Whilst we recognise the benefits of individual pupil logins to our school network, we prefer to use year group logins for ease of access. All members of staff have individual, password protected logins to the school network and visitors to the school can access part of the network using a generic visitor login and password. Supply teachers have a generic supply login and password which is changed regularly. Community users have a generic login and password which is changed regularly.
The school's network can either be accessed using a wired or wireless connection. However, the wireless network is encrypted to the standards advised by **Omnicom** and the wireless key is kept securely by the school office, Computing subject leader and E-safety leader.

School staff, visitors and pupils are NOT permitted to connect personal devices to the school's wireless network. (Exception to this rule will be at the discretion of the Headteacher.)

- Pupils will not use social networking sites (these are blocked) in school and will be educated about their safe usage in their own time. Parents will also be educated in these areas during e-safety workshops.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. **(Reference to YAPPY in KS2 will be made – Your name, Address, Password, Phone number or Your plans).**
- Pupils are forbidden from downloading games or other programmes from the Internet.
- Downloading programs from the internet will be carried out by the IT technician or Computing subject leader.
- Public chat-rooms and instant messaging are **not allowed** and are blocked using the school internet filter.

- Pupils will be educated in 'Information Literacy' and taught how to evaluate the internet content that they have located. Pupils will be taught the importance of crosschecking information before accepting its accuracy.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught to reference materials they have found from other sources so as not to infringe copyright or the intellectual property of others.
- Pupils will be taught how to report unpleasant Internet content.

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by complying with the rules for acceptable computer use, which have been designed to help protect them from exposure to Internet sites carrying offensive material. A most important element of our acceptable computer use agreement for pupils is that they will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable. If there is an incident in which a pupil is exposed to offensive or upsetting material the school will respond to the situation quickly and on a number of levels.

Pupils will be taught to: Report an inappropriate content /image/incident immediately to the teacher. (Without informing their classmates) Teachers will report this to the computing subject leader, E – safety leader or Omnicom.

Procedures for Reporting Inappropriate Content

All staff who believe that an inappropriate item has got through the filter should report it to the Computing leader, E – safety leader or Omnicom immediately. If the matter is non urgent. The IT technician (Omnicom) keeps a log of all reported inappropriate content.

Responding to Incidents

Minor Incidents of Misuse - Pupils

This might include:

- Copying information into projects and failing to acknowledge the source (plagiarism and copyright infringement)
- Downloading materials or images not relevant to their studies, in direct breach of the school's acceptable use policy
- Misconduct associated with logins, such as using someone else's password.

In these most minor of cases the pupil should be issued with a warning by their class teacher, and the incident reported to the, Computing Leader, E – safety Leader or IT Technician (Omnicom)so that documentation is kept. An Incident Log report should be completed by the class teacher (see Appendix D) and passed to the one of the above. If the

behavior is repeated, or the misconduct escalates, it can then be responded to more seriously as there is evidence of previous events. If pupils abuse the privileges of access to the Internet or use of e-mail facilities by failing to follow the rules they have been taught, or failing to follow the agreed search plan when given the privilege of undertaking their own Internet search, then sanctions consistent with our School Behaviour Policy will be applied. This may involve informing the parents/carers. Access to computers and/or the Internet may be denied for a fixed period.

Responding to Inappropriate or Illegal Incidents

It is important that all members of staff – teaching and non-teaching – are aware of how to respond to if an E Safety incident occurs or they suspect a child is at risk through their use of technology. Responding to an E Safety incident in school is no different to responding to other incidents in school.

If an E Safety incident occurs the school will follow its usual procedures for dealing with other incidents including internal sanctions and involvement of parents (for IT, this may include the deactivation of accounts or restricted access to systems as per the school's AUPs (See appendices A - E).

It is very important that appropriate procedures are in place and adhered to for responding to such instances.Our E Safety Leader acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures. Responsibility for handing incidents involving children will be taken by the Designated Person for Child Protection. All the teaching staff will be made aware of the incident at a Staff Meeting if appropriate. Where the school suspects that an incident may constitute a Child Protection issues, the usual Child Protection procedures will be followed.
If a concern is raised, refer immediately to the Designated Person for child protection (Miss Martin). If that is not possible refer to, if necessary, Assistant Headteacher (Mr Andrew) or the Chair of Governors.

It is their responsibility to:

Step 1

Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator.

Step 2

Establish the kind of activity involved and whether it is inappropriate or illegal. If you are in doubt consult the Education Child Protection Service helpline.

Examples of inappropriate activities:

While not illegal, there will be some material that is just not appropriate within the school environment, and, in the case of staff, not in keeping with the professional standards or code of ethics of those who work with children and young people. Some examples are;

- *Deliberately accessing, printing, showing or transmitting inappropriate (or age-restricted) material within the school's network. Even if such material was not deliberately accessed by the pupil, but not reported to a teacher, and was subsequently shown to other pupils, this should also merit a disciplinary response.*

Examples of illegal activities:

In the school context, very serious incidents tend to involve illegal materials (particularly the viewing, possession, making and distribution of indecent images of children) or serious stalking or harassment facilitated by communication technologies. Such criminal offences may be committed by staff and pupils alike.

Some examples are:

- *Indecent images of children are defined under Section 7 of the Protection of Children Act 1978 (as amended by Section 84 of the Criminal Justice and Public Order Act 1994). References to indecent photographs under the Act include data stored on a computer disk or by other electronic means that is capable of conversion into a photograph.*
- *The Protection from Harassment Act 1997 is intended to prevent 'stalking' and other similar unsocial conduct. It states that a person must not pursue a course of conduct which amounts to harassment of another, and which he/she knows, or ought to know, amounts to harassment of the other. Although the term is deliberately not defined in the Act, words such as 'alarm',' distress' or 'torment' fit the term most accurately, and some adverse impact on the victim is required. To constitute a 'course of conduct', harassment must take place on a minimum of two occasions.*

Step 3

Ensure that the incident is documented using the standard child protection incident logging form (Appendix E).

Depending on the judgements made at steps 1 and 2 the following actions should be taken:

Staff instigator – follow the standard procedures for Managing Allegations against a member of staff. If unsure seek advice from the Local Authority Designated Officer or Education Officer.

Staff victim – Seek advice from your LA or Educational Child Protection Service - if it is a child protection issue.

Equally, if the incident involves or leads to an allegation against a member of staff, the school will follow the usual procedures for dealing with any allegation against a member of staff.

Incidents that involve inappropriate but legal material will be dealt with by the school via the usual disciplinary system; unless a criminal offence has been committed, it will not normally necessary to involve the police. Disciplinary action may range from a warning to dismissal of a staff member or suspension of a pupil. As in all disciplinary instances of this seriousness, the school will follow disciplinary protocols, ensuring that proper documentation and recording of information occurs, and that appropriate counselling and support are given, and ensuring that parents and carers of the pupil involved are kept fully informed of the matter.

Discovery of indecent material within the school's network is a very serious situation and must always be reported to the police. The following procedures MUST be adhered to:

- *Evidence must be immediately secured.*
- *The PC concerned must be isolated.*
- *No attempt should be made to investigate the incident – the matter must be referred to the Police to review suspect PCs. Staff should never attempt to access a website which they believe to be illegal – to do so would technically break the law and make them liable to prosecution. If there is any doubt about the subject matter, it is enough to view the Internet history. Any attempt to follow the Internet hyperlinks to the sites themselves will invalidate evidence by updating the time stamps of images received. Material must not be downloaded, printed or sent by email because doing so is an offence in itself.*
- *No member of staff is allowed access to the equipment once this procedure has been implemented.*
- *The school will seek legal advice as soon as possible, particularly with regard to disciplinary actions that are acceptable while the police carry out their investigations.*

Review Following a Serious Incident

In the event of a very serious incident occurring within school, a review of all E Safety policies and procedures will be conducted as soon as possible. The head teacher has ultimate responsibility for the review process, but may delegate this to the E Safety Leader and the school's Computing subject leader. The three key components of a safe ICT learning environment (the infrastructure of whole-school awareness, designated responsibilities, policies and procedures; the effective range of technological tools; and a comprehensive Internet safety education programme) will also be reviewed, ensuring that:

- Comprehensive debriefing occurs after the incident to maximise what can be learnt.
- The ICT technician has the professional skills to carry out regular safety checks, and knows the correct protocols to follow if illegal material is suspected or encountered.
- All school staff understand the circumstances under which a forensic audit of computers should be carried out, and by whom, and the appropriate strategies to adopt to ensure that evidence is secured and preserved.

- The school's E Safety leader and computing subject leader (both policy and management) contains staff with all the relevant expertise, and that the appropriate time and authority is allocated to the team to allow them to carry out their duties effectively.

Acknowledgements

This policy has been drawn up with reference to:

- Signposts to Safety Teaching E Safety at Key Stages 1 and 2 - BECTA (2007)
- Developing a Primary School E Safety Policy - Child Protection Service and Education ICT service (May 2010)

Email

- When available, pupils may only use approved school e-mail accounts on the school. (provided for by the school) Pupils are not permitted to use their own personal email accounts on school equipment.
- Before using school e-mail accounts, children will develop an 'Essential Agreement' with guidelines on how to use email and how to stay safe.
- Pupils must immediately tell a teacher if they receive an offensive e-mail and are asked to keep the email in order to show the adult.
- In e-mail communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mails should be treated as suspicious and attachments not opened unless the author is known.
- Emails 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.
- **Staff should never use personal email addresses to communicate with pupils or parents. An official school email address will be provided by the Computing Subject Leader**.

Photographs/ videos and published content and the school website

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website. **Pupils' full names will not be used anywhere on the Website or Blog, particularly in association with photographs.**
- Work can only be published with the permission of the pupil and parents.
- Pupil image files should be securely stored on the school network.

STAFF WILL BE INFORMED OF ANY CHILDREN WHOSE PHOTOGRAPHS SHOULD NOT BE TAKEN, VIA THE SAFEGURADING BOARD IN THE STAFFROOM.

Parents Taking Photographs / Videos

Under the Data Protection Act (1998), parents are entitled to take photographs of ***their own*** children on the provision that the images are for ***their own*** use, e.g. at a school production. Including other children or other purpose could constitute a potential breach of Data Protection legislation.
Parents are informed that they should only take photographs of their own children and that they need permission to include any other children / adults.

Parents reminded that publishing images which include children other than their own or other adults on Social Network sites is not acceptable, unless specific permission has been obtained from the subjects.

Portable Devices

- **Children will not use mobile phones will not be used during school time and on school property. For children who walk home alone, phones must to be handed in to the class teacher at the beginning of the day. The sending of abusive or inappropriate text messages is forbidden and children are educated what to do in case this happens.**

STAFF MUST NOT USE THEIR MOBILE PHONES IN THE CLASSROOM WHEN THE CHILDREN ARE PRESENT. MOBILE PHONES SHOULD BE KEPT ON SILENT IN A PERSONAL BAG OR LOCKED DRAWER. STAFF MAY USE THEIR MOBILE PHONES DURNING BREAKTIMES AND LUNCHTIME. (IF THERE ARE NO CHILDREN PRESENT)

- Staff should be aware that technologies such as Ultra Portable Laptops, Nintendo DS devices, ipads and tablets and mobile phones may access the internet by bypassing filtering systems and present a new route to undesirable material and communications. Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. **These may not be used in school.**

- Staff should **NOT** use their personal mobile phones to contact pupils or capture photographs of children. Neither should they use personal cameras to take photographs. Alternative equipment will be provided by the school.

Use of personal staff equipment may only be used with permission of the Headteacher.

ALL STAFF MUST TRANSFER PHOTOS/VIDEO TAKEN ON PERSONAL DEVICES ONTO THE SCHOOL SECURE NETWROK WITHIN 24 HOURS. MATERIALS MUST THEN BE IMMEDIATELY DELETED FROM THE DEVICE.

- Pupils are taught how to protect themselves from being victims of identity theft andhow to report such an event to the correct authority.

Social Networks

Social Network sites allow users to be part of a virtual community. Current popular examples of these sites are Facebook, Twitter, Club Penguin and Moshi Monsters (for children). These sites provide users with simple tools to create a profile or page including basic information about themselves, photographs, and possibly a blog or comments. As a user on a Social Network site, you may have access to view other users' content, send messages and leave unmediated comments. Many Social Network sites are blocked by default through filtering systems used in school, but these settings can be changed at the discretion of the headteacher.

Although use of Social Networks tends towards a personal basis outside of the school environment, their use as a tool for communicating with parents is becoming more commonplace in primary schools. Guidance for personal use of social networking, and personal publishing sites is included as part of staff induction, discussed regularly and outlined in the staff Acceptable Use Policy – along with sanctions for inappropriate use.

If a school Social Network page is to be created, you must consider the purpose and audience and also ensure that the privacy settings and interaction are appropriate. **Remember; whatever methods of communication are used, individuals should always conduct themselves in a professional manner. If content is made available on the web it is available for everyone to see and potentially remains there forever.**

All staff need to be made aware of the following points:
The content on Social Network sites may be unmediated and inappropriate for certain audiences.

If a Social Network site is used personally, details must not be shared with children and privacy settings be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.

They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.

The content posted online should not :

- bring the school into disrepute
- lead to valid parental complaints
- be deemed as derogatory towards the school and/or its employees
- be deemed as derogatory towards pupils and/or parents and carers
- bring into question their appropriateness to work with children and young people.

Adults must not communicate with children using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted. Online Communications with parents, past pupils or siblings of pupils, especially if under the age of 18 should be discouraged.

Children must not be added as 'friends' on any Social Network site.

The school will advise parents in terms of their use of Social Networking Sites and how the school will respond to identified issues.

Such as:

- Posting inappropriate comments about staff or children that could be construed as instances of cyberbullying.
- Posting images of children or adults on profiles without permission of the individuals involved, especially if the photographs contain children other than their own.

Protecting Personal Data

- Personal data will be made available to appropriate and approved sources in accordance with the Data Protection Act 1998.

Role and Responsibilities

Our e-safety leader is:
Support will be provided by **Joanne Readshaw** the Computing subject Leader.
Our e-Safety leader ensures they keep up to date with e-safety issues and guidance; keeps the Headteacher, senior leaders and governors updated as necessary; ensures that any e safety concerns are reported in the first instance to the e-safety co-ordinator who will investigate the concern and take the appropriate action.

Our governor responsible for e-safety is:
Our governors have an understanding of e-safety issues and strategies at the school; are aware of local and national guidance on e-Safety; are updated at least annually on policy developments.

Our staff responsibilities are to be familiar with the policy and to adhere to its procedures. They should be familiar with the school's policy in regard to:

- Safe use of e-mail.
- Safe use of Internet.
- Safe use of school network, equipment and data.
- Safe use of digital images and digital technologies, such as mobile phones, digital cameras and iPads.
- Publication of pupil information/photographs and use of website.
- E-Bullying / Cyberbullying procedures.
- Their role in providing e-safety education for pupils.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will always use a child friendly, safe search engine when accessing the internet with pupils (e.g. Google Safe Search – default settings). Staff are to be updated about e-safety matters at least once a year. At the start of each year, e-safety will form part of the staff inset.

Managing Internet Access and Other Technologies

Information system security-

- School ICT systems capacity and security will be reviewed regularly.
- All staff and pupils possess individual logons and passwords to the school network with appropriate access rights and privileges.
- Virus protection will be installed on all school computers and updated regularly in light of new viruses and Trojan Horses that weaken the schools security.
- Staff must ask permission from the e-safety coordinator/computing subject leader before installing software on any school machines.
- Parents' attention will be drawn to the school E-safety Policy in newsletters, the school brochure and on the school website.
- Parents will be given a copy of the Acceptable Use Policy that their child has signed. They will be strongly encouraged and supported to monitor their children's use of technology at home.
- The school will provide regular e-safety sessions for parents.

Glossary

Acceptable Use Policy: A policy that a user must agree to abide by in order to gain access to a network or the internet. In the schools context, it may also cover how other communications services, such as mobile phones and camera phones, can be used on the school premises.

Avatar: A graphic identity selected by a user to represent him/herself to the other parties in a chat-room or when using instant messaging.

Chat-room: An area on the internet or other computer network where users can communicate in real time, often about a specific topic.

Filtering: A method used to prevent or block users' access to unsuitable material on the internet.

Information Literacy: The ability to locate pertinent information, evaluate its reliability, analyse and synthesise it to construct personal meaning and apply it to informed decision making.

Instant messaging(IM): A type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet, analogous to a telephone conversation but using text-based, not voice-based, communication.

Spam: Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

Spoofing: Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a

virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

Trojan Horses: A virus which infects a computer by masquerading as a normal program. The program contains additional features added with malicious intent. Trojan horses have been known to activate webcams, for example, without the knowledge of the PC user.

Virus: A computer program which enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing antivirus software.

All children must sign the AUP before using a school computer.

Appendices to this Policy

Appendix A – Acceptable Use Agreement – pupils

Appendix B – Acceptable Use Agreement – Staff

Appendix C – Acceptable Use Agreement – Guest Users

Appendix D – Misuse of Computer Systems Incident Report

Appendix E – Child Protection Logging Concern Form