E-safety policy

CHAIR OF GOVERNORS: 

Table of Contents

Document History

06/03/15	**"Communications" section updated to include Videoconferencing guidance (JRo)** **"Emerging Technologies" section added (JRo)** **Added 2 bullets points relating to critical evaluation of resources & copyright under "Background / Rationale" section (JRo)** **Updated Appendix B – Staff Acceptable Usage Policy (JRo)** **Added Social Media Policy as Appendix I (JRo)**
15/05/15	**Policy adopted by governors**
07/09/15	**Added additional information based on Prevent awareness**

Background / Rationale

Why is Internet use important?

Education develops and responds to society and the Internet and individual communications are having many effects, some profound, on society.

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is part of the curriculum and a necessary tool for learning.
- Internet access is an expectation for students who show a responsible and mature approach to its use.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries.
- educational and cultural exchanges between students world-wide.
- 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 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 the other schools in the Rowan Learning Trust.
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

Increased computer numbers or improved Internet access may be provided but effective use and quality of learning must also be addressed. Developing effective practice in Internet use for teaching and learning is essential. Teachers will help students learn to distil the meaning from the mass of information provided by the Web. Above all students will learn to evaluate everything they read or see and to take care in their own publishing and interactions with others via the Internet.

At **(add school name here)** High School:

- The school Internet access is designed for student educational use and includes appropriate 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 pupils.

- Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' 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.

How will students learn how to evaluate Internet content?

The quality of information received via media is variable and everyone needs to develop skills in selection and evaluation. Students will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening and how to report it.

More often, students will be judging reasonable material but will need to select relevant sections. Students will be taught research techniques and be encouraged to question the validity, currency and origins of information. Students will compare web material with other sources.

Respect for copyright and intellectual property rights, and the correct usage of published material will be taught.

At **(add school name here)** High School:

- If staff or students discover unsuitable sites, the URL (address), time, date and content must be reported to the Network Manager via the school's IT helpdesk.
- Internet derived materials by staff and by students must comply with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Monitoring of the Policy

The implementation of this policy will be monitored by the Information Systems Manager for the Rowan Learning Trust (who will act as the E-Safety Co-Ordinator) who shall put in place procedures that ensure the school keeps its practices and processes up to date with the rapid changes in technology and use of technology.

The IS Manager shall report termly to the Buildings and Community sub-committee on the operation and implementation of the policy and the procedures developed under it and otherwise on an exceptions basis.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- HHHS monitoring logs of internet activity (including sites visited)
- HHHS monitoring logs of computer usage and keyword flagging
- Surveys / questionnaires of
  - students / pupils (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey)
  - parents / carers
  - staff

A member of the Governing Body has taken on the role of *E-Safety Governor.* The role of the E-Safety Governor will include:

- regular meetings with the Information Systems (IS) Manager
- regular monitoring of e-safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors committee/meeting

The Head of School will ensure appropriate e-safety procedures and processes are in place though the day to day responsibility for e-safety will be delegated to the Strategic Head of ICT and Head of Technologies who shall receive appropriate training and put in place appropriate training for other staff. The Head of School will receive regular monitoring reports from the IS Manager.

Associated Policies

The e-Safety policy is designed to incorporate all ICT policies for the school. Any associated ICT policies are included as appendices to the e-Safety policy, and may be referenced throughout the document.

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is includes incidents of cyber-bullying, or other e-safety incidents covered by this policy and the HHHS Social Media policy, which may take place out of school, but are linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Implementation of the Policy

The IT Support Team are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets the e-safety technical requirements outlined in the HHHS Security Policy and Acceptable Usage.
- that users may only access the school's networks through a properly enforced password protection procedure.
- the school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported effectively.
- that monitoring software/systems are implemented and updated as agreed in school policies.

Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.

- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP).
- they report any suspected misuse or problem to the ICT Helpdesk or IS Manager as appropriate for investigation/action/sanction.
- digital communications with students/pupils (email / Virtual Learning Environment (VLE)/ voice) should be on a professional level and only carried out using official school systems.
- e-safety issues are embedded in all aspects of the curriculum and other school activities.
- students/visitors understand and follow the school e-safety and acceptable use policy.
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor ICT activity in lessons, extra-curricular and extended school activities.
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated person for child protection / Child Protection Officer:

This person should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data.
- access to illegal / inappropriate materials.
- inappropriate on-line contact with adults / strangers.
- potential or actual incidents of grooming.
- cyber-bullying.

Students / visitors:

- are responsible for using the school ICT systems in accordance with the School Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these

issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the school Acceptable Use Policy.
- accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

Education and Training

Students

E-Safety education for students will be provided in the following ways:

- A planned e-safety programme should be provided as part of the curriculum and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Expectations for use of ICT systems/internet will be posted in all ICT rooms.
- Staff will act as good role models in their use of ICT, the internet and mobile devices.

Parents/carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).
The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site.
- Parents evenings.
- Parent awareness events.

Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The IS manager (or other nominated person) will provide advice / guidance / training as required to individuals as required.

Governors

Governors will take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / e-safety / health and safety / child protection.

Emerging Technologies

New technologies are emerging all the time, and many of these offer the potential to develop new teaching and learning tools and methods. The school is eager to embrace new technology where it can have a clear educational benefit, but it is important that any new technologies are assessed for suitability, safety and practicality in terms of monitoring and safeguarding.

The following guidelines will be following when reviewing or introducing emerging technologies

- Emerging technologies will be examined for educational benefit and an assessment will be carried out before use in school is allowed.
- Where appropriate, emerging technologies may be trialled with groups of students/staff before making a final decision. Parental consent should be sought where appropriate.
- Use of any mobile technologies must fall within the behaviour policy and mobile device policy already operating within the school

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the HHHS Security Policy and Acceptable Usage Policy.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- 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.
- All users will be provided with a username and password by the IT Support Team who will keep an up to date record of users and their usernames.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager must also be available to the Head of School and kept in the Head of School’s safe.
- Users will be made responsible 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.

- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and IS manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users' activity.
- An appropriate system is in place, via the IT Service Desk, for users to report any actual/potential e-safety incident to the Network Manager or e-Safety Co-ordinator.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy will be maintained for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- An agreed policy will be maintained regarding the downloading of executable files by users.
- An agreed policy will be maintained regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy will be maintained that makes clear to staff to what extent they can install programmes on school workstations / portable devices.
- An agreed policy will be maintained regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices.
- The school infrastructure and individual workstations will be protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images – Photographic & Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. Staff and students will be made aware of the risks associated with sharing images and with posting digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Students must not, in school, take, use, share, publish or distribute images of others using personal devices.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website (may be covered as part of the Acceptable Use Policy signed by parents or carers at the start of the year)
- Student's work will only be published with the permission of the student and/or parents or carers as appropriate.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

Staff must ensure that they comply with the school Data Protection Policy at all times.

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Students will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Videoconferencing

Videoconferencing enables users to see and hear each other at different locations. It is a real-time interactive technology which has many uses in education. The term videoconferencing extends to technologies such as Skype, and other similar communication tools.

The following steps are taken to ensure the safety and security of students and staff:

- All videoconferencing equipment in the classroom must be switched off then not is use and not set to auto-answer.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact information should not be available on the school website.
- The videoconferencing equipment must be secure and if necessary locked away when not in use.
- Students should ask permission before making or answering a videoconference call.

Specifically relating to computer-based videoconferencing tools.

- Computer-based videoconferencing tools such as Skype should be disabled at the network level and only enabled when there is a specific education need, which has been justified and risk-assessed by a member of staff.
- Students and staff should not use personal accounts when using computer-based videoconferencing. The school will provide such accounts on request.

Videoconferencing content

- Videoconferences should not be recorded without the explicit written permission of all involved parties.
- Any recorded content shall be securely stored.
- Establish dialogue with any third-party providers to ensure the content they will deliver is appropriate and relevant for the students involved.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					✓
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					✓	
On-line gaming (educational)			✓			
On-line gaming (non-educational)					✓	
On-line gambling					✓	
On-line shopping / commerce			✓	✓		
File sharing				✓		
Use of social networking sites				✓		
Use of video broadcasting eg Youtube				✓		

As a Trust we recognise that extremism, exposure to extremist materials and influences can lead to poor outcomes for our students and therefore is addressed as a safeguarding concern. If we fail to challenge extremist views we are failing to protect our children.

As part of a wider safeguarding responsibilities school staff will be alert to:

- Students accessing extremist material online, including through social networking sites.
- Monitor and filter extremist websites and accessing extremist literature.
- Report all concerns to the safeguarding lead at the school.

Responding to incidents of misuse

If there is any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images.
- adult material which potentially breaches the Obscene Publications Act.
- criminally racist material.
- other criminal conduct, activity or materials.

The misuse will be reported to the appropriate authorities by the Head of School.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such incidents the Information Systems Manager will carry out an investigation. The matter will then be dealt with in accordance with the School Behaviour Policy, Staff Code of Conduct and/or Staff Discipline Policy as appropriate.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to SLT	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓		✓	✓
Unauthorised use of non-educational sites during lessons	✓						
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓					
Unauthorised use of social networking / instant messaging / personal email	✓	✓			✓		
Unauthorised downloading or uploading of files					✓		
Allowing others to access school network by sharing username and passwords		✓			✓		
Attempting to access or accessing the school network, using another student's / pupil's account		✓					
Attempting to access or accessing the school network, using the account of a member of staff			✓		✓	✓	✓
Corrupting or destroying the data of other users			✓		✓	✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓				✓	
Continued infringements of the above, following previous warnings or sanctions		✓				✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			✓			✓	
Using proxy sites or other means to subvert the school's filtering system		✓			✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident			✓		✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material			✓		✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			✓			✓	

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓				✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓							✓
Unauthorised downloading or uploading of files	✓							✓
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		✓						✓
Careless use of personal data eg holding or transferring data in an insecure manner		✓						✓
Deliberate actions to breach data protection or network security rules		✓						✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓						✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓						✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✓	✓						
Actions which could compromise the staff member's professional standing	✓	✓						✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓						✓
Using proxy sites or other means to subvert the school's filtering system	✓				✓			
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓			✓			
Deliberately accessing or trying to access offensive or pornographic material	✓	✓			✓			✓
Breaching copyright or licensing regulations	✓	✓			✓			
Continued infringements of the above, following previous warnings or sanctions	✓	✓			✓			✓

Appendix A – ICT Security Policy

Objectives of the Policy

The purpose of this policy is to protect the School's information asset by ensuring:

- Availability: information is and continues to be accessible and usable as normally required.
- Integrity: information is assured with regard to version, accuracy and freedom from corruption.
- Confidentiality: access to information is restricted to the people and for the purposes intended.
- Safety: information can be exchanged in a safe and secure environment for all users

Definition and Classification of Information

Information within this Policy means data, programs, documents, spreadsheets, databases, electronic mail messages, images and maps of all types regardless of how or where within the School the information is stored or managed.

Information Backup

The Information Systems Manager will ensure that appropriate procedures are in place to maintain the confidentiality of the information and to recover from the temporary or permanent loss of the information or supporting equipment.

All information will be protected by a procedure for archiving and copying for secure backup. The procedure will incorporate daily, weekly, monthly, year-end cycles which are appropriate to the type of information, frequency of update, legal and operational requirements.

Security backup copies will be stored, wherever possible, in a physically separate location from the main server room. All backups taken off-site will be encrypted.

Compliance with Legal Requirements

All computer media will be stored and disposed of with due regard to its sensitivity and the requirements of the Data Protection Act.

Disclosure of information will be in accordance with the Data Protection Act, and the Freedom of Information Act.

General Compliance

Unlicensed, illegal or unauthorised software or information will not be installed, used, copied, altered or distributed.

Illegal or improper access to external networks, services or facilities is prohibited.

Access Control

In accordance with section 5 of the Financial Regulations the Director of Finance and IT auditors have access as necessary to any information and applications systems.

Only members of the IT Support team have the access and ability to install and uninstall software.

Any method of log-on which nullifies the password control is prohibited.

Passwords will not be printed or displayed on input.

Each user must only log on with their own user ID and password.

Passwords will be a minimum of six characters and changed in accordance with procedure immediately it is suspected that the password has been disclosed. The change will be to a previously unused password.

Access rights for all leavers will be removed immediately.

Access rights for all users will be reviewed periodically and updated where necessary.

The IT Support Department is responsible for creating new accounts on the network for students and staff. The Network manager will also ensure that new staff have appropriate access rights to both curriculum and admin networks.

The Headteacher is responsible for IT facilities installed within the school and ensuring its proper use. Any use of IT facilities not directly concerned with the school's business is prohibited.

Equipment Physical and Data security.

All items of equipment are security marked (SmartWater) and included in the inventory.

Areas containing ICT equipment will be locked when a member of staff is not present, unless that area has been designated as open-access by the Headteacher.

Terminals and PC's must not be left unattended when logged in to applications. When not in use they will be logged out or protected by a secure screen saver (i.e. locked). Users must log out of the systems and the network before leaving the site and also switch off their terminal/PC.

Personal Systems and Portable PC's

No equipment will be removed from its location without the permission of the Headteacher or Information Systems Manager, who must be satisfied that appropriate arrangements have been made for insurance of equipment and information.

Removal of this equipment will be recorded and monitored.

Equipment must not be left in unattended vehicles for which insurance is not available.

School laptops - there is a separate agreement which all staff issued with a school laptop must sign.

Disposal of Obsolete Computer Equipment

The disposal of obsolete computer equipment is governed by the Schools' Scheme of Financial Administration.

The Governing Body will authorise all writes offs and disposals of surplus stocks in accordance with the school's 'Write off Policy'.

All hard disks will be removed prior to disposal and/or securely wiped beforehand to make the data irrecoverable.

Software will not be offered to an external agency unless there is a legal right to do so and license records are adjusted accordingly.

The inventory will be updated to record disposal.

Appendix B: Staff Acceptable ICT & Internet Use Statement

The computer systems are owned by the school and are made available to staff to enhance their working and professional activities (including routine tasks, administration, management, teaching and research etc). The School e-Safety policy, which this document is a part of, has been drawn up to protect all parties – the staff, pupils and the school. The school also provides internet access to pupils and there is a separate agreement covering this.

The School and The Rowan Learning Trust reserves the right to monitor activities on the school network or computer system, and to examine or delete any files, including emails, that it deems to be inappropriate or in contravention of school policies. All internet access is monitored, and any attempts to access prohibited sites are logged. The school also operates an e-safety monitoring appliance called Securus, which records screenshots of inappropriate activity on staff and students PCs, including staff laptops.

As a member of staff:

- Access must only be made via authorised user accounts, which must not be made available to any other person other than the persons responsible for running and maintaining the system. Workstations should be locked or logged off when leaving a room.

- Under no circumstances should any student be allowed to use a staff account to log into a school computer.

- All Internet use should be appropriate to staff professional activities or student's education needs.

- Internet sites and materials access must be appropriate to work in school. Legitimate private interests may be followed, providing school use is not compromised. For example, finding the results of a cricket match or a weather forecast. Use of the network to access inappropriate materials such as pornographic, racist or offensive material or similar is prohibited. Accidental or unintentional access of such a site should be reported immediately to the school IT Support team, or the Deputy Headteacher, providing the name and web address of the site where possible.

- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden.

- Users are responsible for e-mail they send and for contacts made that may result in e-mail being received. The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded. Posting anonymous messages and forwarding chain letters and spam is forbidden.

- Copyright of materials and intellectual property must be respected.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.

- Staff should not attempt to install software or hardware on school systems without first checking with the IT Support department.

- Staff should consult a member of the IT Support team before purchasing any hardware or software for use on school systems, so that licensing and compatibility with school systems can be verified.

- Staff must take every reasonable precaution to secure any data or equipment removed from the school premises.

- Any equipment taken of site will be the personal responsibility of the member of staff taking it off site. Staff are advised to check that the equipment is covered by a personal insurance policy.

- Violation of the above may result in a temporary or permanent ban on Internet use. Additional disciplinary action may be added in line with existing practise for inappropriate language or behaviour. When applicable, police or local authorities may be involved.

When using the computers and / or internet access with pupils:

Staff are responsible for explaining the rules and their implications to pupils. All members of staff need to be aware of possible misuses of ICT & Internet access and their responsibilities towards pupils. Direct teacher supervision will always be required with pupils using computers and/or the internet. This means a member of staff always needs to be present in the same room being used by the pupils.

Appendix C: Staff Laptop Policy

General Information

- All laptops and accessories remain the property of the school and are on loan to staff whilst they are employed at the school.
- At no time is the laptop the personal property of any staff member. Laptops must be presented upon request and must be returned upon the staff member leaving the school's employment.
- The equipment is listed on the school asset register and is covered under the school's insurance. This insurance covers the use of the laptop at the teacher's home. The insurance does not cover damage / loss in transit between the school and the teacher's home. The laptop must not be left unattended in your vehicle at any time.

Repair and Maintenance

- Any repair and maintenance issues must be reported to the IT Support Department, who will endeavour to solve any issues in a timely fashion. However, should the laptop be out of commission for a length of time, a replacement laptop will be made available wherever possible.
- Staff must not commission a 3rd party to attempt to repair the laptop.

Storage of data

- All staff are reminded that staff wishing to use the laptops to store information, such as student or staff data, should do so only when essential, and under the guidance of the Data Protection Act 1988.
- All staff laptops are encrypted using industry-standard encryption software. Any attempt to remove or circumvent this encryption software is prohibited.

Network Usage

- Laptops that are configured to use the school network may be connected to the school's data infrastructure using any 'live' data socket or a wireless connection.
- The laptops will then have access to the full range of software and services, plus a default printer will be allocated in most cases.
- Laptops should be used within school at least once a month to receive software patches and antivirus updates. This will be performed automatically and will be transparent to the end user in most cases.

Home Usage

- Laptops may be connected to personal Internet connections providing that the Internet connection is protected by a firewall device.
- Staff must be aware that using a personal Internet connection will not provide the same level of filtering or protection afforded by the school Internet connection. Therefore caution should be taken when accessing unfamiliar sites.

- If at any point you believe that the laptop has become infected by a virus of malicious software, you should seek advice from the IT Support department. DO NOT connect the laptop to the school network.
- Limited and occasional personal use of the laptop is acceptable. Any usage must fall within the corporate acceptable use policy for computer use.

Installation of Software

- Staff will be given limited access rights to install software on staff laptops when the laptop is away from the corporate network. These rights will extend to the installation of:
    - Printer software & drivers, and drivers for other peripherals the user may wish to use at home.
    - Antivirus updates for corporate antivirus software.
    - Browser updates and plugins.

  Staff should not attempt to install any other software packages without first consulting the IT Support department. Staff should be aware that staff laptops are regularly audited, and any unauthorised software may be removed without prior notice.

Appendix D: Provision of temporary access for guests

Definition of a guest: Any user who is not employed by the school or Trust, and requires access to school systems to carry out their role. Examples of guests may be:

- Student teachers.
- Supply teachers.
- Council officers.
- Delegates on training courses.

Each guest user will have their needs evaluated individually to determine the exact level of access they require. This will be based on a “start with nothing” principle – guest users will start with no access, and be granted access to the systems they need.

The school operates a “guest” wi-fi network, to which guests may connect their personal devices when appropriate. This network isolates devices, providing them with secure & filtered Internet access but no access to the main school network.

Guests may not connect non-corporate devices to the school network.

Appendix E: Policy for downloading of executable files

This policy acknowledges that executable files are used for many different things and in many guises. For the purposes of this policy, an executable file will be defined as:

- An application / program that can be run directly from the source executable file *or*
- An installable piece of software / software package.

Policy:

- By default, the download of files with executable extension (.exe, .bat, etc.) is automatically blocked by the web filter for staff and students.
- Staff should not attempt to use an executable file to install software onto school PCs – any requests for software install should be made through the IT Support department.
- Users should not introduce executable files onto the school network from any form of removable media (CD, DVD, USB drive etc.)

Appendix F: Remote Access Policy and Guidance

The remote access system allows staff access to specific applications from home. This document details the security prerequisites necessary before access can be granted to individual members of staff. Any staff requesting access must read and agree to this document before being allowed to access the remote access system.

Data Protection

Remote Access will allow staff to access SIMS from outside of school. Because of the sensitive nature of the data held on our SIMS system, staff must abide by the following rules when accessing SIMS via remote access:

- The information must be treated as “for your eyes only”. Other family members, friends etc must not be allowed access.
- Only use the remote access system at home. Don’t log on in a public place or over a public internet connection, e.g. at a wireless hotspot, in a pub/cafe etc.
- Lock your computer if you are leaving the vicinity of your computer for any period of time.
- Do not attempt to save any information to your home computer. Any information accessed must remain on the school systems.
- Make sure you log off securely when you are finished, by following the instructions for logging off in the user’s guide.

Your computer

It is important to make sure that the computer you will be using for Remote Access is secure and free from malicious software, e.g. viruses.

- You must ensure you have up-to-date antivirus software installed on your computer. This software should have the auto-protect feature enabled.
- This antivirus software should be set to run an automatic scan at least once a week, to ensure your computer remains free from viruses and spyware.
- You should ensure that Windows Updates is turned on, and run at least once every fortnight. Microsoft frequently releases patches to fix security problems with Windows, and it is important that these are in place as soon as possible after their release.
- Your home internet connection must utilise a firewall/router device, or you must be running personal firewall software on your home computer.

If you are unsure about any of the above points, see a member of the IT Support department before signing the Remote Access agreement.

Appendix G: Policy for Acceptable Use of Corporate Email

This policy applies to all users who have access to a **(add school name here)** High School email account. By using your email account, you are agreeing to abide by the acceptable usage policies outlined below.

Acceptable

- Communication in connection with **(add school name here)** High School.
- Limited use of e-mail **internally only** for non-school-related purposes **and outside of your working hours.**

Unacceptable

- Customising e-mails such as using non corporate backgrounds, logos or signatures.
- Excessive use of e-mail internally for personal non-school-related purposes.
- Use of School e-mail **externally** for non-business purposes.
- Forwarding chain e-mails.
- Sending school-related information to and from your personal e-mail address.
- Supplying your school e-mail address for non-business related activities, for example Facebook / Internet banking / E Bay / Argos etc.
- Sending unsolicited all-staff emails.

Forbidden

- Sending messages or files that contain discriminatory, abusive, racist, pornographic, obscene, illegal, offensive, potentially libellous or defamatory content.
- Sending personal or sensitive student/school material to employees' personal e-mail accounts, or to unauthorised internal or external recipients.
- Sending emails from another user account **unless specific approval or permission is obtained, which would be granted for example for specific shared mail box management.**
- E mailing confidential, sensitive or personally identifiable information to other people (internal or external) without ensuring that this data is appropriately secured.
- Sending files with non-school related attachments (e.g. compressed files, executable code, video streams, audio streams, or graphical images) to internal or external parties.
- Using web based mail services such as Facebook mail, Google mail etc.

It is important to note that the above lists are not considered to be exhaustive but aim to provide clear guidelines for employees / users.

Appendix H: Policy for School Network and Internet Usage – Students

General use

I will only access the system with my own login and password (where appropriate) which I will keep secret, I will not access other people's files or damage their work and data.

Internet

- I will only use the Internet when I have permission.
- I will use the Internet only for activities and work set by school e.g. homework, class/topic work.
- I will only e-mail people my teacher has approved, and not use the Internet for personal or private messages.
- I will only take part in social networking activities which have been approved by school.
- I will respect the privacy of others. I will not publish their names, addresses, phone numbers or photographs.
- **I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission.**
- I will not use work from the Internet as if it was my own. I will give credit to the sources of materials included in my work.
- I will not try to find or use unacceptable material from the Internet.
- I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself.
- I will not use school resources to subscribe to any goods or services, nor buy or sell using the Internet.
- I will not download software from the Internet.
- I will not bring in floppy disks, CD's or any electronic data from outside the school unless I have been given permission.
- I will not send unsuitable e-mail messages. The messages I send will be polite, responsible and only signed in my name.
- I will not send anonymous messages.
- I will not attempt to bypass the security measures in place on the school network or Internet connection.
- I will not take part in any activity which goes against school rules or government
- I understand that the school may check my computer files and may monitor the Internet sites I visit.

If you have not signed your copy of **Conditions of School's Network and Internet Use** or have had your Internet use removed, or if you do not agree with the policy as listed above, one or more of the following will be enforced:

1. **A temporary or permanent ban on Internet use or computer use**
2. **Additional disciplinary action may be added in line with the school's behavior policy.**
3. **When applicable, parents or other external agencies may be contacted.**

Appendix I: Social Media Policy

A.1. Introduction

(Add school name here) High School recognises that social media is a fast developing area that has the potential to be used to enhance teaching and learning. However as with any new development it is crucial that proper regard is given to the balance between experimenting with new forms of teaching and learning, advancing new forms of communication with students, parents and others, expected professional standards of teachers and above all safeguarding of young people. This policy aims to balance those issues in light of current best practice and the state of technology.

This policy must be read in line with other policies provided by the School, including, but not limited to, the disciplinary and grievance policy, IT policy, safeguarding and all policies relating to discrimination, bullying and harassment.

The protection and welfare of children and young people is the paramount principle in determining how we should act. Accordingly adults should not put themselves, children or young people at risk, should avoid promotion of illegal or harmful activities to children or young people and should demonstrate at all times sensitivity and awareness of the impact of their actions.

You must follow the rules established in this policy in relation to all forms of social media. Failure to comply with this policy could result in disciplinary action which could lead to dismissal depending on the circumstances.

A.2. Definition of Social Media

Social media is a type of interactive online media that allows parties to communicate instantly with each other and allows the sharing of data in a public forum.

Social media covers, but is not limited to, Twitter, Facebook, LinkedIn, YouTube and Flickr.

A.3. Personal use of social media at work

You are not permitted to access social media websites from the School's computers or other electronic devices for personal use at any time.

A.4. Business use of social media

You will be advised by your line manager if you are expected to make use of social media for school purposes and in what forums such use is allowed or not allowed.

If you are unsure about the suitability of a post you wish to make you must discuss it prior to posting with your line manager.

You may contribute to the school's social media activities. You may be requested to provide blogs or articles for publication. Alternatively, if you have something you would like to contribute to the social media controlled by the School please contact your Line Manager.

If you are contacted for comments about the school for publication anywhere, including, but not limited to, social media, educational periodicals or local press, you must discuss

your response with your Line Manager to ensure it is appropriate and compatible with the values of the school.

If you have an idea to use social media to benefit teaching and learning or to improve how the school functions then contact the Strategic IT Manager or relevant member of Senior Leadership.

A.5. Responsible use of social media

If you are required to use social media for school business use remember that you are representing the school at all times and must therefore ensure the communication has a purpose and is intended to benefit the school.

In both business and personal use of social media you must:

a) Have regard to the Teacher Standards 2012 including but not limited to demonstrating consistently the positive attitudes, values and behaviour expected of pupils and students and upholding the public trust in the profession and maintaining high levels of ethics and behaviour both in and out of school. For the avoidance of doubt non-teaching staff are also expected to maintain equivalent standards with regard to social media.

b) Use your common sense before you post anything and think about what you are saying to the world at large.

c) Ensure that you do not post any disparaging or defamatory statements about:
   i) Our school;
   ii) Our staff (current or past);
   iii) Our existing, potential or previous students or parents of students;
   iv) Our suppliers or competitors;
   v) Any person or organisation that has any connection with us.

d) Refrain from posting images or links with inappropriate content;

e) Refrain from breaching confidentiality;

f) Refrain from revealing any trade secrets or confidential information either relating to us or a third party;

g) Refrain from any breach of copyright;

h) Not use social media to bully, harass or discriminate against any party;

i) Refrain from posting offensive religious or political view points;

j) Refrain from entering into contractual arrangements purporting to be on behalf of the school without express permission from your line manager;

k) Refrain from any illegal activity;

l) Refrain from on line fights, personal attacks or hostile postings;

m) Refrain from “friending”, “adding”, “following”, “chatting” or otherwise contacting current or recent students without the express knowledge of and permission from your line manager and only when it is specifically for purposes aimed at improving teaching and learning.

The golden rule - ask yourself whether what you are about to post could cause offence to anyone or be thought inappropriate because teachers are held to higher standards

than most members of the public. If the answer is yes, or you are not sure, then do not make the post.

A.6. Monitoring

If you are allowed to use the school's computers or other electronic devices for personal use the school reserves the right to monitor such use including use of the internet and personal use of social media. Unauthorised or inappropriate use during working hours will result in disciplinary action.

In the event of misuse being found the School may limit your access rights, in addition to any other sanction that may be appropriate.

A.7. Social media in your personal life

The School recognises that many employees use social media in a personal capacity. Whilst you are not acting on behalf of the School, you must be aware that your actions might damage the reputation of your school, your profession and/or your students.

You are allowed to state that you work for the Rowan Learning Trust and/or school, however, your online profile / username must not contain the name of, nickname of or any abbreviations or logos associated with the Trust or the school.

You must not, under any circumstances, use your school email address in any form of personal social media or on the internet at all in your personal capacity. You must set up your own personal email address.

The School discourages you from discussing your working life via social media, however, if you choose to do so remember the **golden rule**. You must not under any circumstances use social media to discuss the actions of, your views about or the performance of any current or past students.

If you believe that your conduct outside of your working life could impact on your professional life think carefully about your privacy settings, consider friend / follower requests carefully giving consideration to who their friends and followers may be, remove tags on photographs or alternatively refrain from the use of personal social media altogether.

A.8. Disciplinary Action

Any breach of this policy may result in disciplinary action being taken against you. Serious breaches of this policy could constitute gross misconduct and could lead to dismissal without notice depending on the circumstances of a particular case.

The School reserves the right to require you to remove a posting from any social media forum and any failure to comply with this request may constitute an act of gross misconduct for failing to follow a reasonable management instruction.

A.9. Reporting of incidents

If you become aware of any colleague failing to comply with this policy or if you have failed to comply with this policy you must report it to your line manager immediately. If

the failure to comply relates to actions by your line manager then you must report it to a member of the senior leadership team at your school.

Line managers should report incidents further using their professional judgment. Where a posting, link or other technical issue requires immediate removal, blocking or other appropriate technical action the Strategic IT Manager should be informed immediately.

A.10. Remember the golden rule

Ask yourself whether what you are about to post could cause offence to anyone or be considered inappropriate given your professional role. If the answer is yes, or you are not sure, then do not make the post.