RISHWORTH SCHOOL: E-SAFETY POLICY including:

Review Initiated by	*PSe /ASG*
Reviewed	*Michaelmas 2016*
Next Review	*Michaelmas 2018*

Appendix 1: Staff Acceptable Use Agreement
Appendix 2: Pupil Acceptable Use Agreement

Distribution: Website, Policy Library on the Network.

Introduction and Responsibilities

The internet and the use of digital media, is an essential part of education in the 21st Century. It is our aim as a school to provide appropriate and safe access to all that the internet and modern technology allows through the provision of modern and up-to-date ICT facilities. Responsibility for this safe provision is as follows:

- The Headmaster and Head of Heathfield have overall responsibility for e-safety within the school.
- The DSL (Heathfield and Rishworth) responsibilities for safeguarding apply equally to online behaviour as they do to all other behaviour.
- The ICT Support Manager has delegated responsibility for ensuring that the network and computer systems are used appropriately by all users and that safeguarding systems are fully functional.
- The ICT Committee will help form and monitor e-Safety policy and strategy.

Access to, and the effective use of, the internet within education, business and social interaction is an essential element of modern life. The internet is a rich resource for all sorts of information and its appropriate use should be encouraged to enhance teaching and learning. Increasingly pupils turn to the internet in the first instance in their search for resources or information. In addition, the internet is an important source of services used in everyday life, such as banking and social networking. Equally, it plays an important role in the administration of the school.

Alongside these opportunities there are risks attached its use. Distribution of material cannot be controlled. Once posted to an initial target audience, material can be posted anywhere through the networks of each individual in that audience and beyond.

It is important to ensure that we consider the above in line with our duties in School, as well as our legal responsibilities and our reputation. It is also important that we encourage an understanding that online activity is subject to all of the norms, protocols and regulations that apply to relationships in “real life”.

The intention of this policy is to set out the ways in which the school will provide access to the internet with a view to ensuring staff and pupils are able to do this safely.

Internet Access for Teaching, Learning and School Administration

"Young people need to be able to determine which websites or other sources of information are reliable and which are bogus; to understand the dividing line between 'fun' and 'inappropriate' behaviour; and to grasp the risks they take in posting the pictures or comments online which they may come to regret, if not now then as adults and job-seekers in the future". (ASCL, The Impact of ICT, 2020 Future: Briefing Paper 4.)

- School internet access is designed expressly for staff and pupil use and will include appropriate filtering.
- Clear boundaries are set for the appropriate use of the internet and digital communications through Acceptable Use Agreements.
- Pupils are taught to be critically aware of the materials they read and are educated in the effective use of the internet for research, including the use of discrimination in the search for information and its retrieval. They are shown how to validate information before accepting its accuracy.
- Pupils are educated that the use of internet derived materials by staff and by students must comply with Copyright Law

Managing Internet Security

- The security of the School's ICT system will be reviewed regularly by the ICT Support Manager.
- Virus protection is installed and regularly updated.
- Security strategies will be discussed at least annually by the ICT Support Manager and senior staff.

Use of E-mail

- Pupils should speak to a member of staff or their parents should they receive anything that is or which they consider to be offensive in whatever form (ie picture, comment telephone message etc) by text, e-mail or any other digital medium.
- Staff are all issued with a school e-mail address, the use of which is encouraged for the smooth running of the school. All staff should be aware of the School e-mail Policy which defines safe and appropriate use.

Social Networking

- The school will control access to social networking sites via the school network and educate students in their safe use. Social networking sites will not normally be accessible unless a specific use is approved.
- Students will be given e-safety guidance on safe internet use both in and out of school. This will include:

1. Advising pupils that they should not generally give out personal details which may identify them, their friends or their location.
2. Advising pupils and staff that they should not place personal photos on any social network space without considering how the photo could be used now or in the future.
3. Advising pupils and staff that they should only invite known friends and deny access to others when using social networking and instant messaging services.
4. Making pupils and staff aware of the need for security and the importance of setting passwords to deny access to unknown individuals and to block unwanted attention and communications.
5. Making pupils and staff aware of the Child Exploitation and Online Protection Centre (NCA's CEOP Command) and the 'Report Abuse' links that exist on most social networking sites.

Published content and the school web site

- Staff or student personal contact information will not generally be published. Any contact details given online should be those of the school office.
- The Headmaster will take overall editorial responsibility and ensure that published content is accurate and appropriate.
- The School reserves the right to include photographs and images of pupils in the school's promotional material. We would not disclose the name or home address of a child without the parents' consent. Parents who do not want their child's photograph or image to appear in any of the school's promotional material must make sure that their child knows this and should write to the Headmaster to this effect or complete the photographic consent form that is in the Parent and Pupil Handbook. This policy is consistent with the Terms and Conditions that all parents agree to when their son or daughter joins the school.
- Photographs that include pupils will be selected carefully with a view to our responsibilities for their safety and well-being.
- Work produced by pupils may be published on the website and in other school publications.

Managing Filtering

- The school will work in partnership with its providers to ensure that systems to protect pupils are regularly reviewed and improved as necessary.
- Staff and pupils will be encouraged to report any unsuitable website or web content that they discover to their form teacher or a teacher that they trust so that the ICT Support Manager can act on the information.
- The ICT Support Manager is responsible for ensuring that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable and take account of statutory responsibilities such as the need to protect children from radicalisation.

Managing Emerging Technologies

- Emerging technologies will be examined for their educational benefit and assessed before use in school is allowed.
- Technologies such as mobile phones with internet access are not part of the school network and are able to bypass school filtering systems and present a new route to undesirable material and communications. It is not possible to monitor this activity with the resources that are currently available to the school and it is not the school's policy to prevent pupils from bringing their own 'phone' which tends to include these facilities into school. The school will nevertheless revisit this regularly and as technology develops.
- The sending of abusive or inappropriate text messages and images are likely to be unlawful and will be treated seriously.
- Tablets or mobile phones may only be used during lesson or formal school time when permission is given by a member of staff.
- Games consoles may only be used in school with permission.

Protecting Personal Data

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

Policy Decisions authorising internet access

- Staff must agree to the Staff Acceptable Use Policy in order to use the computer network.
- Pupils must agree to the Student Acceptable Use Policy in order to use the computer network.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Parents will be asked to sign the Student Acceptable Use Policy when their child joins the school, to show that they understand and are in agreement with the terms of usage.
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of internet access, although it will do all that is reasonably possible to reduce the risk of inappropriate material being accessed.
- The Headmaster and the Head of Heathfield will ensure that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of internet misuse by pupils will be referred to the Head of Section / Deputy Head at Rishworth and the Deputy Head at Heathfield, in the first instance.
- Any complaint about internet misuse by staff will be referred to the Headmaster or Head of Heathfield in the first instance or the Deputy Head where the Headmaster or Head of

Heathfield are not available. The Bursar will deal, in the first instance, with any complaint about the misuse of the internet, by support staff.

- Complaints relating to safeguarding will be dealt with in accordance with the school's child protection procedures.

<u>Communicating E-safety</u>

In order to create an environment where E-safety is instinctively known and understood we intend to educate the whole-school community. In this we include parents and governors.

Pupils

- E-safety information will be posted in rooms where computers are used.
- All users will be informed that network and internet use is monitored.
- Pupils will be warned about the misuse of the school system including the search for and use of proxy websites to circumnavigate the measures put in place to ensure safe and appropriate internet access.
- A number of staff will be CEOP trained in both schools. They will advise on e-safety matters and deliver e-safety training to staff and pupils through classroom sessions as well as other forums such as assemblies.
- A programme of training in E-safety will be delivered across the whole school through the curriculum and more broadly, as appropriate to age and section, making use of appropriate materials, e.g. those from CEOP.
- The Acceptable Use Policy and the Student Planner will include advice on how to stay safe on the internet.

Staff

- All staff will be made aware of the school's e-safety policy.
- Staff will be informed that network and internet traffic is monitored and can be traced to the individual user.
- Staff will receive e-safety training on a regular basis.
- Colleagues that manage filtering systems or monitor ICT use will be supervised by senior management and will work to clear procedures for reporting issues.
- The policy is not intended to restrict all employee activity on social media however school representatives are asked to exercise caution and professional judgement about what they use it for, who they communicate with and subject matter. Colleagues are advised to make full use of the security settings available within the systems but note that these cannot be guaranteed to provide protection against allegations being made or disciplinary action being taken. The school considers having pupils and current parents as 'friends' on social networking sites to be problematic and something that might very easily compromise a member of staff professionally or impact upon the School's reputation. It is, therefore, the school's strong advice that staff should not have current parents or pupils as 'friends' in this environment.

Governors

- The Board of Governors is aware of the School's e-safety policy and strategy which exists with its approval.
- Governors will be attend and receive e-safety training as members of the school community. This will be refreshed as appropriate.

Parents

- Parents will be made aware of the school's e-Safety Policy through school publications and mailings.
- Relevant e-safety material will be made available to parents with a view to educating them as members of the wider school community and with a view to ensuring safe use of the internet at home as well as in school.
- Information meetings may be arranged to supplement the information made available to parents as appropriate.

Related policies and documentation

Anti-Bullying Policy
Promoting Good Behaviour
Child Protection and Safeguarding Policy
E Mail Policy
ICT Acceptable Use Agreements (below)

Sources:

BECTA
NCA's CEOP Command
www.getsafeonline.org
Childnet, ThinkuKnow
Julia Codman, CEOP and Sheffield Safeguarding

Appendix 1: Staff Internet and Network Acceptable Use Policy

This forms part of the Staff Behaviour Policy

1. Introduction

1.1 This policy sets out the general rules for the use of Rishworth School's internet and network systems by its staff.

1.2 This applies to all staff at the school which includes:

- Rishworth School, Heathfield Junior School and Rishworth Sport's Club staff
- Any temporary member of staff, peripatetic staff or visitor using a guest account on the school system.

1.3 All users have a responsibility to use school's computer resources and the internet in a professional, lawful and ethical manner. Abuse of the computer network or the internet, may result in disciplinary action, including possible termination, and civil and/or criminal liability.

1.4 Effective security is a team effort involving the participation and support of every Rishworth School employee and affiliate. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

1.5 The school's network and internet systems are coordinated and managed by the Information and Communication Technology (ICT) Support team.

1.6 All members of staff are expected to promote responsible and lawful use of the internet and school network resources.

1.7 The content of this policy is to be reviewed with new members of staff during the relevant induction process.

2. General guidelines

2.1 School computers, internet access and e-mail are provided to **support pupils and teachers** in the pursuit of their **academic studies** and to allow efficient communication and access to information for **educational purposes**.

2.2 The efficient working of the computer network depends on the good sense and co-operation of all users. In using the system staff agree to the policy and guidelines included in this document

3. Guidelines for the use of the School Computer network:

3.1 All material stored in a member of staff's user area is their responsibility. Log-in details must be kept secret and immediately changed if compromised.

3.2 Accessing or attempting to access another user account without that user's permission or good cause must not occur.

3.3 Internet and e-mail facilities must be used responsibly. The school network should not be used to search for, store or pass on inappropriate images or information. This includes material that advocates illegal acts, discrimination, or violence towards other people.

3.4 Social networking sites (Facebook, Instagram etc) should not normally be accessed through school computers.

3.5 The school's e-mail protocol should be used as a guide in all communications and in particular with regard to those with parents and pupils.

3.6 The school has a responsibility to provide a safe environment for members of the community to use the internet and e-mail facilities. The school must also comply with the law. For this reason restrictions do apply to certain sites. Users should not attempt to circumnavigate the school web filtering system. In such instances contact the ICT department and access, where appropriate, will be enabled.

3.7 Software and programmes must not be put onto the school network without reference to the ICT Support Manager.

3.8 The school has a duty to provide a safe environment for all users. For this reason be aware that the use of the school network is monitored.

4. In line with this guidance and with a spirit of creating a safe learning environment to work and teach within proscribed use of the internet includes:

4.1 Visiting internet sites that contain obscene, hateful, pornographic, radicalised or extreme political views or otherwise illegal material;

4.2 Using the computer to perpetrate any form of fraud, or software, film or music piracy;

4.3 Using the internet to send offensive or harassing material to other users on any basis, especially gender, race, age, disability, religion, sexual orientation or national origin;

4.4 Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under an agreement or other such licence and authorised;

4.5 Using the school internet facilities for gambling purposes;

4.6 Hacking into unauthorised areas;

4.7 Publishing defamatory and/or knowingly false material about Rishworth School, Heathfield Junior School, your colleagues or students on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format;

4.8 Revealing confidential information about Rishworth School in a personal online posting, upload or transmission - including financial information and information relating to our students, policies, staff and/or internal discussions;

4.9 Undertaking deliberate activities that waste staff effort or networked resources;

4.10 Introducing any form of malicious software into the school network;

4.11 Making contact with students through social networking sites;

4.12 The use of anonymous proxies is forbidden.

5. Blogging

5.1 Blogging by employees, whether using Rishworth School’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of Rishworth School’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not bring the school into disrepute and is not detrimental to school’s best interests, and does not interfere with an employee's regular work duties.

5.2 Employees are prohibited from revealing any Rishworth School confidential or proprietary information when engaged in blogging.

5.3 Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the school and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.

5.4 Employees may also not attribute personal statements, opinions or beliefs to Rishworth School when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the school. Employees assume any and all risk associated with blogging.

5.5 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Rishworth School’s trademarks, logos and any other school intellectual property may also not be used in connection with any blogging activity.

6. Virus detection

6.1. Files obtained from sources outside the school, including disks brought from home, files downloaded from the internet, cloud based storage, newsgroups, bulletin boards, or other online services; files attached to email, and files provided by customers or vendors, may contain dangerous computer viruses that may damage the school's computer network. Users wishing to transport work files on CDs/DVDs, memory sticks or other portable storage media are responsible for ensuring that they are free of viruses. If you suspect that a virus has been introduced into the school's network, notify the ICT Support Manager immediately, do not however forward a file suspected of containing a virus to the ICT support team or any other user.

7. Frivolous Use

7.1 Computer resources are not unlimited and are provided expressly for the purposes of teaching and learning. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources for their primary purpose. As such, the user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the internet.

8. School-owned information held on third-party websites

8.1 All work stored on school servers and school provided cloud based storage remains the property of Rishworth School. Sensitive or confidential information should not be synchronised to third party storage websites. This includes information stored on third-party websites such as web based file hosting and social networking sites, for example; Facebook, Google Docs, LinkedIn, OneDrive or Dropbox.

9. Portable Media used for file transportation

9.1 If users are transporting important documents using portable media, they should password protect files or make use of encryption tools or hardware. Users should NEVER have in their possession the personal details of children or colleagues.

9.2 Users should always ensure they have a backup of any documents stored on portable media.

10. File sharing Networks and Peer to Peer

10.1 Participation in distributed file-sharing networks is not permitted under any circumstances. This means that file sharing programs (including BitTorrent, Kazaa, Gnuella, Foxy, eDonkey, WinMX, 4onDemand, BBC iplayer Download Manager, Limewire, PPStream, Thunder and Thunder5) should never be used on the school's network. However, BBC iplayer video streaming is allowed. If in any doubt whatsoever, please refer to the ICT Support Manager.

10.2 This point specifically relates to peer-to-peer networking activity, it has no bearing on sharing resources in Google Docs.

11. Usage Monitoring

11.1 Under the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the school reserves the right to monitor and record internet usage patterns. The school can monitor and record internet usage. However, the ICT Support team does not routinely inspect internet usage for staff, but may inspect any or all files that are stored on school resources to the extent necessary to ensure a compliance with the school policies and procedures. The school reserves the right to do this at any time, but will not conduct covert monitoring except in exceptional circumstances, such as where there are grounds for suspecting criminal or equivalent malpractice. Such inspection of files requires the authorisation of the Headmaster or Bursar. Users should not have an expectation of complete privacy as to his or her internet usage.

12. School network passwords

12.1 Each user is required to create a password, bearing in mind complexity rules that apply on the school system; all users must use the following guidelines for creating your password:

- Passwords must be at least eight characters long.
- Passwords may not contain your user log on name or your name.
- Passwords must contain characters from at least three of the following categories:

a) English upper case letters -	eg: A, B, C, … Z
b) English lower case letters -	eg: a, b, c, … z
c) Numbers -	eg: 0, 1, 2 … 9

d) Non-alphanumeric (“special characters”)
eg: Punctuation marks and other symbols

12.2 Passwords must never be disclosed to other users. It is recognised that from time to time your line manager may need access to your logon account or access may required from a maintenance perspective.

12.3 Passwords must be changed on a 90 day basis – once a password has expired, the user will be denied access to webmail/outlook web access, 3Sys/PASS, TOPdesk, Room Booking System and Google Apps, until a new password is set in school.

12.4 Users are encouraged to use random passwords and not just increment a number at the end of the password.

12.5 You can change your school network password at any point using the Control + Alt + Delete keys to access the facility on a PC keyboard.

12.6 Out of school passwords can be changed in outlook web access, however if a password has already expired a new one has to be set from a PC within school.

13. Logging off and correct power down of equipment

13.1 Users are required not to leave screens logged on, unattended.

13.2 Consideration should be given to other users and ensure screens are correctly logged off after use and not left locked.

13.3 At the end of the day PCs should be logged off correctly and powered down. The school is committed to the conservation of energy as well as extending the life of owned equipment.

13.4 Teaching staff working in ICT rooms; during the last period of a day are responsible for ensuring all PCs in the room are powered off correctly at the end of the lesson, this can be done easily using the Crosstec Schoolvue facility.

13.5 Teaching staff are responsible for ensuring classroom projectors are powered down at the end of each day and when not in use for long periods. eg: over the lunchtime period.

14. Roaming Profiles

14.1 Roaming profiles allow a user to log on to any computer on the same network and have a consistent desktop experience, such as applications remembering toolbar positions and preferences, or the desktop appearance staying the same. All staff are provided with roaming profiles to facilitate the log on process and ensure settings within the likes of Microsoft Outlook are moved around the school when staff logon in different locations. An icon is shown in the notification area, to the bottom right of the taskbar to indicate to the user the remaining free space in the profile.

14.2 There is a restriction of 60mb attached to all roaming profiles, a user cannot exceed this limit and should try to ensure the profile is kept to half this size.

14.3 If a user exceeds the limit for a roaming profile it will not allow them to logoff, without reducing the size of their profile.

14.4 Ensuring the roaming profile is kept as small as possible ensures we reduce slowness in logging on the system.

14.5 In the interest of keeping profiles as small as possible users should not save files and folders on the desktop, shortcuts to files and folders should always be used instead.

14.6 Pictures used for desktop background should always be low resolution.

15. User areas

15.1 All users are provided with a user area, this is a data storage area to support work appropriate to the individual, rather than a group of users in a department.

15.2 Individual user areas are mapped to ‘Documents’ in the Windows 7 operating system when the user logs on.

15.3 Individual user areas should never be used to store; collections of photographs, video or music, personal or school related.

15.4 Photographs, video and music files appropriate to the school must be stored in an appropriate shared area to ease archiving off the system on an annual basis. Files of this nature are only kept on the system for a period of 12 months.

15.5 Users should ensure that data no longer required in their individual user areas is cleared out on at least an annual basis.

15.6 Any files stored in the school’s ICT system are the property and responsibility of the school.

15.7 Users are not permitted to save files to the local C: drive of a PC or laptop.

15.8 No provision is provided for users to save personal data on the school system.

16. Google Apps for Education (GAFE)

16.1 All staff members are provided with access to a Google Apps account, this is a collection of resources that are an aid to teaching and learning at Rishworth School. It provides an easy method to transfer documents between home and school, provides easy collaboration; allows for sharing of resources between the teacher and student or vice versa, and other colleagues. This allows you to work anywhere on whatever device.

16.2 Access to the Google Apps system is provided using your usual school network user name and password.

16.3 Access must only be made via the user's authorised account and password, which must not be given to any other person.

16.4 Neither Google nor Rishworth School guarantee security of any data stored within your Google Apps account.

16.5 Confidential data must not be stored using this facility.

16.6 Copyright and intellectual property rights must be respected.

16.7 The Google Apps facility provided by Rishworth School may not be used for private purposes.

16.8 The security of your Google Apps account must not be compromised.

16.9 Irresponsible use may result in the loss of access to your Google Apps account.

16.10 Access to your account will be removed along with all data stored on leaving the school.

17. Length of file names

17.1 Microsoft Windows limits file names to 256 characters. The user should consider the total number of characters permitted, this includes the folders etc. that make up the actual file path and spaces. (For example; C:\Program Files\filename.docx).

17.2 File names greater than the maximum character length can result in the content becoming corrupt, the content may not be accessible and risks backup software not saving the files. The best (and safest) practice is to use the shortest reasonable file name possible.

17.3 Punctuation should be avoided when creating folder or files names. You can't use any of the following characters in a file name: \ / ? : * " > < |

17.4 The use of any punctuation in a file name can cause unexpected results when trying to open files, copying them or backing up or trying to restore the file.

18. Boarding staff living on-site

18.1 At the discretion of the Bursar a PC or laptop may be provided to the Head of boys and Head of girls boarding staff living on site to enable connection to the school network in on-site accommodation, this is to support their job at the school.

18.2 No connection to school domain can be provided for personal equipment.

18.3 An internet connection on the boarders' network can be provided for personal equipment, providing up to date antivirus software is installed.

18.4 To facilitate freedom of surfing the internet and total privacy for staff living on-site, they are encouraged to provide their own internet provision.

18.5 If wireless access points are used in staff boarding accommodation; the SSID should be hidden and access password protected with a minimum of 128 bit encryption. The configuration of any access point must not interfere with school equipment.

18.6 With the exception of software covered by the Microsoft Work at Home licensing agreement, no provision is available to provide other school owned software.

18.7 The ICT Support team are not responsible for any aspect of maintaining personal equipment.

19. Laptop users

19.1 Users of school laptops provided to support the employee's job are responsible for ensuring these are reconnected to the main school network once a week to ensure anti-virus protection is updated from the school server.

19.2 School laptops are not a substitute for a users home computer, no administration access is provided to allow installation of the users own choice of software etc.

19.3 Periodically the ICT support team may ask for the laptop to be brought in for maintenance purposes or for updating. If the laptop is found to be storage for a user's personal photograph or other media collections these will be removed.

20. Visitors

20.1 Visitors are not permitted to connect personal equipment; including PCs, Laptops, Netbooks, MacBook's, Tablets (including iPads), mobile phones, games consoles or wireless access points to the main school network, for internet access.

20.2 A visitor or contractor to the school site can be provided with a guest logon to use with school equipment.

20.3 Please provide the ICT Support Department with reasonable notice via the TOPdesk system (at least 24 hours) that a visitor may require access to the system and the level of access required. In some cases the ICT Support Manager will seek permission from the Bursar before allowing such access.

21. Printing

21.1 All users have a responsibility of looking at ways to reduce printing costs, this may be achieved by:

- Ensuring bulk printing is sent to cost effective shared printing resources.
- Ensuring print matter is collected from print rooms.
- Making use of print and then release later methods on multi-function copiers rather than sending documents to print from remote locations and not collecting the material. (This includes setting release passwords on documents sent.)
- Publishing and sharing files and documents internally on shared areas or externally amongst the Rishworth School community on Google Apps, rather than printing.

21.2 Departmental costs for network printing are provided to Heads of Department on a half termly basis.

22. Software

22.1 No user is permitted to install software on school PCs or laptops.

22.2 Software can be installed by providing the ICT Support Manager the software title and the appropriate licensing documentation. No software title will be installed without production of correct licensing documentation.

22.3 The ICT Support Manager reserves the right after evaluation to refuse a request to install freebie software.

22.4 The school has 2 preferred internet browsers; Microsoft Internet Explorer and Google Chrome; these are installed by default on all PCs across the school site. The use of different browsers is a matter of personal preference and in a school environment we cannot take into consideration personal preference.

22.5 Users can be provided with a Microsoft Office 2010 disk for installation at home under the terms of the Microsoft Work at Home licensing agreement. (Please see Appendix I of this documentation.) The ICT Support team have no responsibility for problems that may occur from the installation of any school provided software.

22.6 Providing software titles for installation at home is dependent on the software license agreement purchased by the school.

22.7 The ICT support team maintains a log of all authorised and licensed software used on site for external inspection if required. Any software used on site which has not been logged by the ICT Support Manager jeopardises the school’s position with licensing authorities and the user may be disciplined under the school’s disciplinary policy.

23. Personal equipment

23.1 Under no circumstances are users permitted to connected personal equipment; including PCs, Laptops, Netbooks, MacBook’s, Tablets (including iPads), mobile phones, games consoles or wireless access points to the main school network.

23.2 The ICT Support team have no responsibility for maintaining any aspect of personal equipment.

24. ICT Assistance

24.1 ICT support is available between 8.30am and 5.00pm by logging requests with the ICT team using the TOPdesk facility. Support requests logged are prioritised by the ICT Support Manager. In the event of urgent requests the ICT Support Manager should be contacted direct via mobile phone; however the request will still need to be recorded on the TOPdesk system as a record of the work being undertaken.

24.2 The ICT Technician can be contacted via mobile phone outside normal working hours in the event of total system failure (access to network drives are not available across the school or main school internet failure) or in the aftermath of a major power failure. Internet problems are more often than not a problem with the internet service provider or BT and therefore the length time the internet is down is beyond our control.

24.3 In the event of an out of hours call out being necessary the ICT Technician should be contacted either by the Head of boys or girls boarding or a member of the Senior Management. The ICT Technician will give an indication as to when he is able to attend the site.

24.4 The ICT Technician will need to attend the site in the event of power being off on the site for longer than 15 minutes.

24.5 The ICT team can support presentations providing that the appropriate room has been booked correctly and sufficient advance notice is provided.

24.6 In the event of special presentations out of normal hours – during an evening or weekend (eg: New parent’s morning, Sixth Form open evening, Boarders’ Induction) the ICT Technician can be contacted by mobile phone for any assistance with equipment.

25. Misuse

25.1 Misuse of the internet and network in line with this policy and these guidelines may be dealt with under the School’s Disciplinary Procedure.

Appendix I: Microsoft Volume Licensing – Work at Home Agreement

As part of our Academic licensing agreement with Microsoft we have a 'Work at Home' agreement.

What is Work at Home licenses for Academic Volume License Customers?
Academic institutions that have acquired licenses through Microsoft Academic Volume Licensing programs may grant to their staff the right to use a second copy of a limited selection of products on either a home or portable computer for work-related purposes.

The school must make reasonable efforts to ensure that faculty, staff, or other employee users delete and remove such copies from the temporary RAM and permanent memory (in other words, the hard disk) of their computers at the end of the agreement term.

Which selection of Microsoft Products qualifies under the work at home agreement?
The limited selection of Microsoft products in our case refers to Microsoft Office; it does not apply to operating system software.

Distributing software for Work at Home rights
We have Work at Home licenses available through Microsoft Academic Volume Licensing, access to media by employees must be restricted and regulated. All media for software distributed for Work at Home use must be acquired from a Microsoft-approved fulfilment source. Software may be distributed to employees in the following way, only:

> *We purchase a download of the software and a product key is allocated to an authorised employee. The facility is setup through our Authorised Education Reseller (AER) and we can purchase product keys not exceeding the total number of licensed users. You cannot duplicate Work at Home software. eg: Software copies and product keys cannot be passed on to other users. We purchase these licenses at an approximate cost of £7.15 + VAT per user. Each user gets a personalised product key for installing the software and cannot be re-used for another user. Software is provided to a user for installation on a single PC only.*

We cannot provide employees with a copy of the original installation CD, because of copyright infringement and we should not provide anyone the school's main license product key. If we provided the main license key to employees each installation is activated online, should the product key be passed on to others then it will eventually leave us with a problem in activating MS Office installations in school.

We must make every effort to ensure the installation of the software is controlled and removed from the home PC when the employee leaves Rishworth School. There should also be some form of disclaimer that says we are not responsible for any problems that may occur from using any installation provided by the school. Below is the agreement form which staff must complete before any software is issued.

The cost for providing the licensing will be charged to the appropriate department and refunded once the media and product key is returned on expiration or termination of the agreement.

Rishworth School

Microsoft® Academic Open License Staff – Work at Home Licensing Acceptance Form

This acceptance form is valid for the Microsoft products checked below, which shall be referred to collectively herein as the "Software". Software is made available to you because Rishworth School has purchased software licenses for the Software through a Microsoft Academic Open License agreement. Rishworth School is extending to you the right to use the Software for **work-related** purposes at home. **You are not licensed to use the Software at home for personal purposes.** You do not own the license, the Software, or the CDs. You will be required to remove the software from your home machine at the time of agreement expiration or termination.

Work at Home Use Rights have been granted by Rishworth School for the following product(s (referred to collectively herein as the "Software"):

❑ Microsoft Office Professional Plus 2010

Please initial each statement:

____ I will read and abide by the license agreement associated with this software.

____ I understand that no technical support is provided by Rishworth School in association with my work-at-home use.

____ I understand the minimum specifications to run the Software as listed at http://www.microsoft.com/products.

____ I understand that I must remove the Software from my machine at the time of agreement expiration or termination and provide confirmation that this has taken place.

____ I understand that I am not licensed to use the Software for personal purposes.

____ I understand that the software supplied or any product codes cannot be passed on to any other user.

____ I understand that the software provided can only be installed on a single PC.

Employee signature: _________________________

Printed name: _______________________

Date: ___________

When extending Work at Home rights to your licensed users, Rishworth School must make reasonable effort to ensure that employees delete such copies from their computers at the end of the agreement term. Employees wanting to take advantage of work at home licensing must accept the terms of the Academic Open License agreement and sign the acceptance form before media is distributed. The completed form should be returned to the ICT Support Manager.

Employees must recognise that Rishworth School are not responsible for the installation of the software detailed above on home equipment, no responsibility can be accepted for the update or maintenance, ongoing or otherwise of such equipment or any problems that may occur from the installation of products provided by the school.

Media Supplied Date: ___________________________

Product Code: ____

Appendix 2: Student ICT Acceptable Use Agreement

General guidelines:

- School computers, internet access and e-mail are provided to support pupils in their **academic studies** and to allow efficient communication and access to information for **educational purposes**.
- Computer use and internet access are privileges, not rights, and access requires responsibility. The efficient working of the computer network depends on the good sense and co-operation of all users. In using the system, I am accepting this principle.

Guidelines for the use of the School Computer network:

1. I will keep the details of my log-in secret and not allow others to use it. All material stored in my user area is my responsibility. I will change my log-in details immediately if I believe they have been compromised.
2. I agree to respect the privacy of other users on the network. I will not try to discover their log-in details or access, delete, modify or use documents contained within their user area unless expressly authorised or directed to do so by a member of staff
3. I will use the internet and e-mail facilities responsibly. I agree that I will not use the school network to search for, store or pass on inappropriate images or information. This includes material that advocates illegal acts, discrimination or violence towards other people.
4. I will not use the internet in order to bully, insult, intimidate or victimise individuals within or beyond the bounds of our school community. Social networking sites may not be accessed through school computers, unless authorised by a member of staff.
5. I accept that the school has a responsibility to provide a safe environment for members of the community to use the internet and e-mail facilities. The school must also comply with the law. For this reason restrictions do apply to certain sites. I agree that I will not attempt to circumnavigate the school web filtering system and that any attempt to do so will rightly be seen as premeditated and will mean that I am attempting to access material or sites that are strictly forbidden.
6. I understand that playing web-based games is not allowed because of the impact they have on the efficient running of the system. Educational games can be used when instructed by a member of staff.
7. I agree that I will not attempt to load software onto the school network. I also agree that I will not introduce or develop programmes that may harm the overall integrity and security of the school network.

8. I agree that I will not use the school computers for the purpose of buying, selling or gambling.

Personal Safety:

In order to ensure that all users are safe whilst using the school network we ask you to respect the following rules and guidelines:

1. Unless required in class as part of an ICT activity, I will not put my or any other person’s personal information on the internet. This includes such things as names, addresses, contact information, school or work addresses.
2. I understand that it is unwise to contact or communicate with people that I do not know over the internet. It is not always possible to establish whether or not the person introducing him/herself is who they seem to be. Should someone try to contact me I agree that I will inform a member of staff immediately. I will **never** agree to meet anyone that I have met over the internet without my parents’ approval or without taking a responsible adult with me.
3. I will be respectful and use appropriate courtesy and language in all communications. If I receive any communication that contains offensive language, or which makes me feel uncomfortable, I will inform a member of staff immediately.
4. The school wants to provide good computer facilities to support the pupils and students within its community. In doing this it has a duty to provide a safe environment for all users and for this reason I understand that the use of the school network is monitored.

If I fail to do this:

- I may be banned from using the facilities temporarily or permanently.
- The Headmaster, My tutor, Head of School Section and Parents/Guardians will be informed and action, disciplinary or otherwise, taken in accordance with appropriate policy: in severe cases this may lead to a requirement to leave the school
- If it is applicable, the Police may become involved.

Google Apps for Education (GAFE)

All students are provided with access to a Google Apps account, this is a collection of resources that are an aid to studies at Rishworth School. It provides an easy method to transfer documents between home and school, provides easy collaboration; allows for sharing of resources between the teacher and you or vice versa, as well as you and other students. This allows you to work anywhere on whatever device. All of the **Guidelines for the use of the School Network** (above) apply to your use of Google Apps, however, you should be particularly aware of the following:

1. The Google Apps system is accessed using your usual school network user name and password.
2. Access to Google Apps must only be made via the user's authorised account and password. You must keep the details of your log-in secret and will not allow others to use it. All material stored in Google Apps on your user area will be your responsibility. You will change your log-in details immediately if you believe they have been compromised.
3. Neither Google or Rishworth School guarantee security of any data stored within your Google Apps account.
4. Personal or confidential data must not be stored using this facility.
5. Your Rishworth School Google Apps account should be used for educational purposes and things related to your learning. Private or personal information should not be stored on Google Apps. It is really important that you keep your private information separate from School.
6. Unsafe or inappropriate use of Google Apps may result in the loss of access to your account.
7. When you leave the School access to your account will be removed along with all data stored on your Google Apps account.

E-mail usage

All students have access to the school email system via outlook web app using their network user name and password. The student email system is monitored for potential misuse and as such should not be regarded as private.

The system is accessible from inside and outside school by typing the following into the address bar in an internet browser: http://www.rishworthstudents.co.uk/webmail

The email system should be used only for educational purposes.

- You should not give away personal or confidential information
- Unasked for or junk email must not be sent, forwarded or encouraged.
- Emails should be used for a positive reason and must not contain material which is in any way likely to offend or to distress others.
- Email addresses are provided to enhance your learning experience so it is important that messages are meaningful. You should ensure that attachments are appropriate to your learning.
- Your school email address must not be given to an external organisation when making personal purchases.

Plagiarism

Plagiarism is intellectual theft. This means that you use someone else's work or ideas but pass them of as your own. The most common way that someone commits plagiarism is by doing research on the internet and cutting and pasting things that interest them into a project of piece of work without properly crediting the work to the original author. Apart from being very lazy, plagiarism is a very serious offence because it is theft and if you were to plagiarise someone's work in any exam work the exam board can give you zero for your work and ban you from getting any grades in **any** of their specifications. Where plagiarism is suspected, the school will investigate the matter fully and in addition to any decision that the Board might make will treat the matter very seriously.

How can I avoid plagiarising someone's work?

If you find something that is useful to you for a project you can use the material that you find selectively but you need to properly credit the author (say who wrote the material and where you found it). You should not be tempted to try and copy and paste huge amounts of text and data.

Rishworth Post

Rishworth Post is our communication system which brings together email, text messaging, secure web-based access to documents, and online reply and consent forms into a single comprehensive package. It is an inclusive system which is available parents, staff and pupils. All students are provided with secure access to Rishworth Post.

Rishworth Post may be used to allow students to see trip information and forms sent out to parents, to provide students with information sent out about the school or to allow students to see published external examination results.

Useful tips

1. Creation of school network passwords

Password complexity rules apply on the school system; please use the following guidelines for creating your password:

1. Passwords must be at least eight characters long. Current thinking within the ICT industry recommends that three unrelated words create a powerful password e.g. Dublinsofadaffodil1
2. Passwords may not contain your user log on name or your name.
3. Passwords must contain characters from at least three of the following categories:

   a) English upper case letters - eg: A, B, C, … Z

   b) English lower case letters - eg: a, b, c, … z

   c) Numbers - eg: 0, 1, 2 … 9

   d) Non-alphanumeric ("special characters") eg: Punctuation marks and other symbols

You can change your school network password at any point using the Control + Alt + Delete keys to access the facility on a PC keyboard.

All users of the main school network are required to change their password on a 90 day basis. Out of school your password can be changed in outlook web access, however if a password has already expired a new one has to be set from a PC within school.

2. Saving your work

a) It is useful to create folders in your home directory on the school server for storing files. For example, create an ICT folder for storing work done in ICT lessons and so on.

b) Choose file names that relate to or describe the file contents. eg: ‘Castles Homework’ rather than just ‘Homework’.

c) Backups of your work are created at the end of each school day, but it is also advisable to create a backup for yourself on your USB memory stick.

d) There are limits set on the amount of data that can be saved in your user directory on the school server, this is for school work only and the space should be used wisely.

e) On leaving the school work saved in your user area will be archived for a period of six months. Once this period has passed, the folder and contents will be deleted.

Rishworth School

Student Acceptable ICT Use Policy

Agreement

STUDENT:

I have read and understand the Student Acceptable ICT Use Policy and will abide by it.

STUDENT'S FULL NAME:

SIGNATURE:

STUDENT'S FORM:

DATE:

I have read and discussed the content of this ICT agreement with my son / daughter.

PARENT'S FULL NAME:

SIGNATURE:

DATE: