Reading School: ICT User Agreement Return Form (AUP)

For clarity, please use block capitals

Student First Name		**Year started at Reading School ?** …………………………………….
Student Last Name		
Tutor + Group	**Current Year Group**	**House**
	7 8 9 10 11 12 13	**C E S W**

	Please circle to confirm…
I have read the User Agreement attached to this return form	**YES**
I have read the E-Safety Policy on the school website*	**YES**
I have read the Social Networking Policy on the school website*	**YES**
Are you a Boarder at Reading School?	**YES NO**
If you are a boarder which Boarding House are you in?	**South House** **East Wing**

*www.reading-school.co.uk/70/safety

User Agreement:

- I understand and I agree to abide by the conditions listed in the attached agreement.
- I understand that if I break this agreement, access to all ICT facilities, both networked and stand-alone, will be immediately withheld pending investigation.
- I understand that any disciplinary action taken against me may, in extreme circumstances, result in my exclusion or dismissal from the school and the possible involvement of the police.

	Signature	***Date***
Student Signature:		
Parent Signature:		

Please detach this page from the User Agreement.
After completing please sign and return to the School Office.

ICT User Agreement (AUP)

Contents

Philosophy 3

Duty of care & e-Safety 3

Personal security 3

Use of the school ICT equipment 3

Agreement Conditions 4

Using the Internet 5

E-mail 6

Cyber bullying & Whistleblowing 6

Social networks, blogs and Twitter 6

Internet Access for pupils in the Boarding Houses 8

Monitoring & Tracking ICT Use 8

Printing facilities 9

Data protection 9

Sanctions 9

Philosophy

At Reading School we believe that the use of Information and Communication Technology prepares pupils to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology, both off and online. Pupils use ICT tools to find, explore, analyse, exchange and present information responsibly, creatively and with discrimination. They learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of people, communities and cultures. Increased capability in the use of ICT promotes initiative and independent learning, with pupils being able to make informed judgements about when and where to use ICT to best effect, and consider its implications for home and work both now and in the future.

The overall aim for the informed use of Information and Communication Technology at Reading School is to enrich learning for all pupils, to support their academic studies, pastoral care and recreational interests and to promote effective communication.

Duty of care & e-Safety

Reading School has a duty of care towards every member of the school to ensure the safe use of computing facilities. New members of the school are asked to read and agree to the rules for the acceptable use of the school computer network that follow and sign to indicate that they have done so. All staff undertakes online e-safety training and all students are encouraged to act responsibly at all times and to be aware of the issues of “content, conduct & contact” when they use ICT, both in school and at home.

This acceptable use agreement applies without exception to all members of the school at all times and to visitors with temporary access. It is assumed that by logging into a school computer or by accessing any of the school's ICT services you are agreeing to abide by this agreement.

Further information can be found in the policy documents on the school website (E-Safety Policy, Social Network Policy for Students and Social Network Policy for Staff).

Personal security

The security of your own files is your own responsibility. Do not give anyone your password and get it changed it if you think someone else has discovered it. Every member of the school has a responsibility to protect the security and confidentiality of the school computer network.

Do not give your password to anybody.

Use of the school ICT equipment

Access to the school computer network must only be made using an authorised account username and password. Your individual account should be used to store all your work and is available from any terminal in the school.

Your personal folder must regularly be cleared of unnecessary files.

All computer equipment is security marked and machine serial numbers are logged. Computers and their peripherals are all property of the school and must not be moved or removed from the premises without permission. Work may be shared or exchanged with others using the appropriate folders on SharePoint or other online spaces set up by individual departments for that specific purpose.

Agreement Conditions

These conditions apply without exception to all members of the school at all times, irrespective of location, and includes visitors with temporary access.

1. Reading School provides ICT facilities to all students and staff who have been registered with the curriculum network manager by signing and returning their ICT Agreement. As a registered user you may use any these facilities in order to carry out your work, to store files in your own user area on the network, to send and receive emails and to access appropriate information on the Internet.
2. You cannot use any ICT facilities until you are registered and have signed the conditions for use agreement. These conditions are necessary for one or more of the following reasons:

   a. To ensure that all equipment, peripherals, curriculum or administration networks and internet access function properly and are thus available for the benefit of registered users at all times
   b. To ensure that information stored by staff and students is kept safe and available at all times
   c. To comply with the appropriate laws governing the use or misuse of ICT and internet facilities
   d. To ensure that the school and its staff can carry on with their day to day business effectively

3. You should be aware that by signing this agreement you give consent to the network managers and other ICT staff, in the normal pursuit of their work, having access to your user area, your files, to your e-mails. You should also be aware that the time and dates of your network usage are logged and all websites you have visited on the Internet are logged and can be examined. If you break the conditions of the agreement you may be liable to sanctions, up to and including exclusion from the school.

When using Reading School ICT facilities you MAY:

4. Use the facilities for your schoolwork or for other appropriate work.
5. Send personal e-mails outside of lessons using only the Webmail email system provided with your login account. The sending of emails during lessons, other than class work related messages, is not allowed.
6. Access the Internet providing this does not prevent anyone else from carrying out their work and that such activity falls within the conditions for the use of the facilities.
7. Store only such files as are needed for your work

When using Reading School ICT facilities you MAY NOT:

8. Send electronic communications which could bring yourself or the school into disrepute or which could render yourself or the school liable to prosecution
9. Knowingly access, view or download any material capable of giving offence
10. Keep, or pass on, e-mails received which contain material capable of giving offence
11. Knowingly import programmes, download files or open attachments that cause viruses to be spread
12. Add to the programs already available to you, either on the network or a stand-alone machine. This includes accessing or downloading games and other programs either from the internet or from other external storage devices (including flash drives, hand held devices, mobile phones or similar)
13. Leave yourself logged in. When away from your station, you must logout
14. Give your password to any other person or allow them to use your account.

15. Attempt to gain the password of or access the work area of another user
16. Take part in any other computer related activity which could give offence or bring yourself or the school into disrepute or render yourself or the school liable for prosecution
17. Attempt to change the operation of any ICT facility by amending its configuration settings, except with the express permission of the network managers or the head of ICT or under instruction of those acting on their behalf
18. Connect any equipment or devices (including flash drives, hand held devices, mobile phones or similar) to any ICT facility, except with the express permission of the network managers or the head of ICT or under instruction of those acting on their behalf.
19. Attempt to circumvent any security systems in place or to be knowingly party to such attempts, either before or after the event.
20. Attempt to log into a computer using another person's credentials or attempt to log in as a system administrator.
21. Become involved in any inappropriate, antisocial or illegal behaviour involving the school computer systems.
22. Send offensive or harassing material to others or take part in any form of cyber bullying.
23. Use school computer equipment for any commercial purpose.
24. Never tamper with or vandalise school computer equipment or attempt to install software.
25. Never connect your own computer hardware or mobile device to the school network without permission.
26. Never unplug a school computer or disconnect its network cable.
27. Never create or store files that contain unsuitable or offensive language or images.
28. Never download or attempt to use any unauthorised executable files on the network.
29. Never commit copyright violations, such as illegal copying of music files, movies, pictures or software.
30. Always notify a member of the ICT department if you identify a problem or witness unacceptable behaviour.
31. Any activity that threatens the integrity of the school computer systems, or that hacks, attacks or corrupts the network, is forbidden.

Using the Internet

All members of the school have access to the internet, for educational purposes. Internet content is filtered and your internet access is monitored and the websites you visit are logged. Online games are forbidden and some social networking sites may be blocked during the school day – others may be accessible for classroom work. Any use of any social network site, during lesson times, must be classwork related and with the agreement of supervising teacher.

Never:

32. Attempt to access inappropriate websites or material by trying to circumvent the school internet filtering system.
33. Create, share, store, download or display any offensive, obscene, indecent or menacing images, stories, data etc.
34. Engage in any commercial activities online.
35. Use the school computer systems for political purposes or advertising.
36. Promote or provide instructional information about illegal activities or promote physical harm to anything or anyone.
37. Use peer-to-peer services within school
38. Upload, download or attempt to spread any computer virus.
39. Use the school's facilities to attempt to gain unauthorised access to any other computer systems.
40. Use any technique which would disrupt network communication, security or integrity.

If you are unsure about the suitability of a web page, close the page and consult a member of staff immediately or report the website to the ICT department using the support@reading-school.co.uk email address. Give the URL of the website and a brief note about why you are reporting it.

You should be aware of the implications of copyright and and the consequences of plagiarism – any passage of text, copied from a public source such as the internet should be acknowledged, giving the site URL and, where appropriate, the name of the author and date.

E-mail

E mail is a vital business and educational tool, but an informal means of communication. Give consideration to the appropriate use of language in your e mail messages. In general, try to write an email as professionally as you would a letter. In general you:

41. Should check your school email account regularly: at least once per day.
42. Should attempt to respond to or acknowledge e mail messages reasonably quickly.
43. Are responsible for the content of all emails you Send, Forward, Reply To or Reply All to and for any contacts you make.
44. Should NOT provide your address, telephone number, bank account number, credit card details or photograph as part of an email unless the recipient is known personally.
45. Should always remember to use the Bcc: field when you write an email with multiple recipients, to keep your recipient’s email addresses private.

Never use email on a device connected in any way to the school facilities to:

46. Transmit obscene, hateful or threatening communications.
47. Communicate or publish defamatory or racially offensive materials
48. Communicate or publish defamatory or homophobic materials.
49. Transmit via email any unsolicited advertising, junk mail, spam, chain letters, or any other form of email solicitation.
50. Use the email system to commit crimes or to bully, harass or stalk others.
51. Use the school email system for personal financial gain, gambling, political purposes or advertising.

Cyber bullying & Whistleblowing

Behaviour that is of a bullying nature is never acceptable, either online or offline. Cyber bullying refers to the use of information and communications technologies to victimise, threaten, tease or harass others. Mobile phone text messages, e mail, phone calls, internet chat rooms and instant messaging and social networking websites can all be misused for cyber bullying.

If you wish to report inappropriate behaviour you can speak to any teacher or other member of staff or, if you wish, you can email them. You can also find advice on the CEOPS website by clicking on the icon on your desktop.

Social networks, blogs and Twitter

The use of social networking websites in school time is discouraged and access to acceptable sites is limited to certain times of the school day. Most social networks and communication tools such as Twitter have age restrictions.

The school and some individual departments and teachers have blogs and Twitter accounts and these can be used in school. When interacting on a school blog or Twitter account always be careful what you post; it will be monitored and moderated if necessary.

Never:

52. Post anonymous messages, personal remarks or personal details about anyone else or impersonate someone else.
53. Use photographs of groups or individuals on a website or blog without their permission.
54. Post or respond to electronic communications or messages that are impolite, indecent, abusive, discriminatory, homophobic or racist or in any way intended to cause hurt to another person.
55. Post personal information about yourself, such as your age, hobbies, phone numbers or your address or post code.
56. Post anything that could be considered upsetting.
57. Be derogatory to any person or bring the school name into disrepute.
58. Use the internet or email to arrange to meet someone you do not know - not everyone is who they say they are

Internet Access for pupils in the Boarding Houses

Reading School has a special duty of care towards its boarding community to provide a safe, secure and healthy environment in which to live and work. Wireless Internet access is available in the boarding houses and all reasonable precautions have been taken to make sure that the Internet access provided is safe and secure, but the onus is on boarders to use it responsibly.

Housemasters are conscious of their duty of care towards the boys with regard to adequate sleep and development of social skills. The excessive use of laptops or hand held devices can be a cause for concern and Housemasters will exercise their duty of care when necessary in this regard.

In addition to all previous rules that apply at all times throughout the school the following specific rules apply to the use of personal computer equipment (BYOD) in the boarding houses:

59. With consent from parents and housemasters, boarders in Years 10 and above may bring their personal computers, tablets or mobile devices into the boarding house (this does not apply to mobile phones which any boarder may bring).
60. Boarders in Years 10 and above who have the consent of their parents, housemaster and permission from the network manager, may use the wireless network.
61. Your laptop or device must never be connected into the main school network.
62. You are permitted to use the guest wireless network, following discussion with your House Master.
63. Your laptop or device must have up-to-date antivirus software installed
64. You are wholly responsible for your actions, or the actions of any other user you permit to use your laptop or device.
65. You are responsible for ensuring that your laptop or device is stored securely when it is not being used.
66. You are responsible for maintaining your own computer equipment.
67. No direct technical support, software or maintenance should be expected from the school's ICT department.
68. Do not leave equipment switched on when unattended for any period of time.
69. You are responsible for ensuring that any important work is backed up regularly.
70. The school must be given permission to carry out physical inspections of equipment, including electrical safety testing, and, when breach of this user agreement is believed to have occurred, examination of the contents your equipment, including any storage devices.
71. Boarders are expected to stop using all forms of electronic equipment at lights out.

Content filtering is relaxed after school, except during prep time, to allow some recreational use of the internet and access to approved sites. Requests for particular sites and sources to be unblocked should be made to the ICT department and will be considered, as long as they do not affect the safety and security of our school systems. All recreational use of the internet at all times, and in all instances, must be legal and must not be liable to bring the school into disrepute in any way.

Monitoring & Tracking ICT Use

The school, through the ICT department, has the right to openly monitor the use of computer equipment and internet and email systems to prevent them being used inappropriately, for unlawful purposes or to distribute offensive material, balanced against an individual users right to privacy. Administrators reserve the right to examine, use and disclose any data found on the school's networks for the purposes of ensuring the health, safety, discipline or security of any student or staff member or to protect property. This information may, if necessary, be used in disciplinary actions.

Printing facilities

The school has excellent printing and photocopying facilities but printing, especially colour printing, can be very costly and wasteful. You can save time & money and reduce waste easily:

72. Print more than one page per sheet of paper or print double sided.
73. Use more of the page by changing your document margins and remove blank pages.
74. Print straight to a photocopier instead or print one copy and photocopy it.
75. Email it, or share your work using SharePoint or some other appropriate shared storage system.

Data protection

The Data Protection Act, (1998), states that organisations which store personal information must register and state the purpose for which they need the information. Reading School is registered as a 'data controller' under the data protection act to store reasonable information about its pupils and staff.

Sanctions

Depending on the severity of the offence and at the discretion of the Teacher, Housemaster or Headmaster (or whoever is dealing with the case), one of the following will apply:

76. Temporary ban on internet or network use.
77. Permanent ban on internet use.
78. Permanent network ban.
79. Normal school disciplinary action.
80. Police involvement, where appropriate.