

Acceptable Use Policy

Independent Day / Boarding School for Boys and Girls

Royal Hospital School

January 2010

1 Scope

- 1.1 This policy has been authorised by the Governors and is addressed to all pupils. It is available to parents on request and parents are encouraged to read it. The policy takes into account Becta guidance: *AUPs in Context: Establishing Safe and Responsible Online Behaviours* (AUPs: Acceptable Use Policies) and *Cyber-bullying: safe to learn: embedding anti-bullying work in schools* (DCSF00658-2007), guidance issued by the Department for Children Schools and Families. The policy relates to the use of technology, including:
- 1.1.1 e-mail;
 - 1.1.2 the internet;
 - 1.1.3 Virtual Learning Environments;
 - 1.1.4 social networking or interactive web sites for example Facebook, Bebo, MySpace;
 - 1.1.5 instant messaging, chat rooms, blogs and message boards;
 - 1.1.6 gaming sites;
 - 1.1.7 mobile phones;
 - 1.1.8 mobile phones with the capability for recording and/or storing still or moving images;
 - 1.1.9 webcams, video hosting sites (such as YouTube);
 - 1.1.10 personal music players such as iPods;
 - 1.1.11 handheld game consoles;
 - 1.1.12 SMART boards;
 - 1.1.13 other photographic or electronic equipment.
- 1.2 It applies to the use of any of the above on school premises and also any use, whether on or off school premises, which affects the welfare of other pupils or where the culture or reputation of the School are put at risk. Staff are subject to a separate policy which forms part of their contract of employment.

2 Aims

- 2.1 The aims of this policy are:
- 2.1.1 to encourage pupils to make good use of the educational opportunities presented by access to the internet and other electronic communication;
 - 2.1.2 to safeguard and promote the welfare of pupils by preventing "cyberbullying" (see 3.1 below) and other forms of abuse;
 - 2.1.3 to minimise the risk of harm to the assets and reputation of the School;
 - 2.1.4 to help pupils take responsibility for their own e-safety (see 3.2 below); and
 - 2.1.5 to ensure that pupils use technology safely and securely.

3 Definitions

- 3.1 **Cyberbullying** is the use of information and communication technology (ICT), particularly mobile phones and the internet deliberately to upset someone else.
- 3.2 **E-safety** means limiting the risks that pupils are exposed to when using technology, so that all technologies are used safely and securely.

4 Protocols

- 4.1 Pupils should comply with the following protocols:
- 4.1.1 e-mail and internet protocol (Appendix 1);
 - 4.1.2 mobile phone protocol (Appendix 2);
 - 4.1.3 camera, photograph and video protocol (Appendix 3);
 - 4.1.4 other electronic equipment protocol (Appendix 4);
 - 4.1.5 protocol for communication between staff and pupils (Appendix 5).

5 Sanctions

- 5.1 Where a pupil breaches any of the School's protocols, the Headmaster will apply any sanction which is appropriate and proportionate to the breach including, in the most serious cases, expulsion. Other sanctions might include: increased monitoring procedures, detention, withdrawal of privileges.
- 5.2 **Confiscation:** unacceptable use of electronic equipment could lead to confiscation in accordance with the protocols attached to this policy and the School's policy on Behaviour and Discipline.

6 Procedures

- 6.1 Pupils are responsible for their actions, conduct and behaviour on the internet in the same way that they are responsible during classes or at break time. Use of technology should be safe, responsible and legal. Expulsion is a possible consequence for any pupil found to be responsible for material on his or her own or another website that would be a serious breach of school rules in any other context. Any misuse of the internet will be dealt with under the School's Behaviour and Discipline Policy. If you witness misuse by other pupils **talk to a teacher about it as soon as possible.**
- 6.2 Pupils must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anti-bullying Procedures. If you think that you might have been bullied or if you think another person is being bullied, **talk to a teacher about it as soon as possible.**
- 6.3 If there is a suggestion that a pupil is at risk of abuse, the matter will be dealt with under the School's Child Protection Procedures. If you are worried about something that you have seen on the internet, **talk to a teacher about it as soon as possible.**

7 The liability of the School

- 7.1 Unless negligent under the terms of this policy, the School accepts no responsibility for loss to the pupil or parents caused by or arising out of a pupil's use of mobile phones, e-mail or the internet whilst at school.
- 7.2 The School does not undertake to provide continuous internet access. E-mail and website addresses at the School may change from time to time.

8 Monitoring and review

- 8.1 All serious e-safety incidents will be logged by the Deputy Headmaster.
- 8.2 The Deputy Headmaster has responsibility for the implementation and annual review of this policy. The Deputy Headmaster will consider the record of e-safety incidents and new technologies. The Deputy Headmaster will consider if existing security procedures are adequate.

Authorised by	Resolution of the Board of Governors
----------------------	--------------------------------------

Date	20 January 2010
-------------	-----------------

Effective date of the policy	20 January 2010
-------------------------------------	-----------------

Circulation	Governors / all staff / parents / pupils on request
--------------------	---

Appendix 1

[Pupils' handbook]

E-mail and internet protocol

Introduction

- 1 We want each pupil to enjoy using the internet, and to become proficient in drawing upon it both during your time at school, and as a foundation for your further education and career.
- 2 However, there are some potential drawbacks with e-mail and the internet, both for you and for the School.
- 3 The purpose of this protocol is to set out the principles which you must bear in mind at all times and also the rules which you must follow in order for all pupils to use technology safely and securely.

Principles

- 4 For your own protection and that of others, your use of e-mail and of the internet will be monitored by the School. Remember that even when you have deleted an e-mail or something you have downloaded, it can still be traced on the system. Do not assume that files stored on servers or storage media are always private.
- 5 Passwords are there to protect users. It is a serious offence to use the username and password of another user. Users should not reveal their password to any other user, not even an administrator or member of staff. A user whose account has been disabled by an administrator must apply to an administrator to have the account enabled at times when it is needed for lessons. Impersonation of another user via e-mail is a serious offence. All of your files should be saved in your own area.
- 6 The use of e-mail and access to the internet from the School's computers and network must be for educational purposes only, during School hours. You must not use our facilities for personal, social or non-educational use during School hours without the express, prior consent of a member of staff.
- 7 You may only use e-mail and access the internet once you have received IT induction training. If, at any time after that, you are unsure whether you are doing the right thing, you must ask for help from a member of staff.
- 8 You must do all you can to protect the security of the School's computer network, and the security of networks belonging to others. In particular, this means being aware of the possibility of computer viruses and taking sensible precautions to avoid bringing them onto our system or passing them to others. You should tell a teacher if there is a failure in a technical safeguard e.g. if there is a problem with a firewall or if an area which should be password protected is not password protected.
- 9 You must also try to protect personal and confidential information about yourself and others, even if you receive or come across this inadvertently. Receiving or using this kind of information may be unlawful under data protection legislation and laws relating to confidentiality.

- 10 You must not knowingly obtain (or attempt to obtain) unauthorised access to any part of any computer system, or any information contained on such a system, including the School's system. This is known as "hacking" and is both a criminal offence and a serious breach of school discipline.
- 11 You should assume that all material on the internet is protected by copyright and you must treat such material appropriately and in accordance with the owner's rights - you must not copy (plagiarise) another's work.
- 12 You must not create, display, copy or otherwise distribute offensive material. Offensive material includes but is not limited to racism, sexism, pornography, bullying (including homophobic bullying), defamation, blasphemy or criminal activity including hacking. In cases of doubt, please ask any member of staff. As far as you are able, you must also make sure that you do not search for or receive such material. It is your responsibility to reject it if you come across it, and to inform a member of staff. Do not store executable files (.exe. files) or other copyright material such as MP3 files, wallpapers, movie clips and other formats or movie clips in your user area.
- 13 You must not bring the School into disrepute through your use of e-mail, mobile phones or your access to the internet. For example, you must not send or ask to receive anything which you believe the School and/or your parents would find inappropriate for a pupil at The Royal Hospital School.
- 14 You must not enter into any contractual commitment, whether for yourself or on behalf of The Royal Hospital School.
- 15 You will also be liable to disciplinary sanctions including, in the most serious cases, expulsion, if you breach this protocol. The measures taken will depend on the seriousness of the offence. Normally a verbal warning will be issued for a minor misdemeanour but further sanctions may be taken against those who repeatedly offend or where the nature of the offence is more serious. You (or your parents) may also be asked to pay for any significant expenditure, or indemnify any significant liability, incurred by the School as a result of the breach.
- 16 It is a serious offence to destroy work (files) of another user, or to create or introduce a virus or other malicious code to cause a system malfunction. Users must not attempt to reconfigure the computer, place shortcuts, aliases, software or Clip Art onto any local hard disk. Programme files must not be downloaded from the internet. Personal floppy disks, USB pen drives and CD ROMs containing application software must not be brought into school. However, pupils may bring in work on floppy disks or USB drives, if approved by staff beforehand.
- 17 You should treat all ICT resources responsibly, and avoid waste by not sending documents to print unless you have first previewed them, and are sure they are in final draft form. Colour printing is permitted, but pupils are expected to use this facility sparingly and not print off web pages unless absolutely necessary. All colour printing is monitored.
- 18 Pupils are not allowed to access peer-to-peer interactive or networking web sites when using school computers or, if using personal laptops or other devices, on school premises, during School hours.

Rules

- 19 You may only use the School's computers whilst logged on with your own username and password.

- 20 You must never disclose your password to another pupil, nor to anyone outside the School.
- 21 You may send and receive e-mail and have access to the internet at school only during term time and only during the school day. The School will not forward e-mails received during the school holidays.
- 22 You may not read anyone else's e-mails without their consent.
- 23 You must not send an e-mail to an entire address list or distribution list without the express, prior consent of a member of staff.
- 24 You must not use web based e-mail accounts such as Yahoo, Hotmail or USA.NET. This will be unnecessary as you are provided with your own personal e-mail account. You can access your Royal Hospital School e-mail from home.
- 25 You may not send or receive e-mail messages, attachments or program files greater than 250 megabytes.
- 26 You must tell a member of staff immediately if you have accidentally read, downloaded or have been sent inappropriate material, including personal information about someone else.
- 27 You must not load material from any disk, USB memory stick or storage device (such as an MP3 player or PSP) brought in from outside the School, unless the device has been virus checked.
- 28 If you think or suspect that an attachment sent to you, or other material which you want to download, might contain a virus, you must not open the attachment or download the material without first speaking to a member of staff to arrange a virus check.
- 29 You must not cancel or disapply the School autosignature / disclaimer attached to all e-mail messages.
- 30 You must not send or receive encrypted messages. If you receive any encrypted messages these must be referred to a member of staff.
- 31 No 'laptop' or other portable devices may be connected to the School network without the consent of a member of staff.

Appendix 2

[Pupils' Handbook]

Mobile phone protocol

- 1 All pupils are forbidden to use or carry mobile phones within School hours for any purpose, including texting, phoning, taking still or moving images, checking the time, using Bluetooth, using as a calculator or surfing the internet. Day pupils must hand in mobile phones when they arrive at School to senior house staff.
- 2 All pupils may use mobile phones within the boarding house at those times prescribed by the Senior House Staff, which will not include prep time or during the hours between which the pupil is expected to be in bed.
- 3 Senior House Staff will store the mobile phones of those pupils below the Sixth Form and issue them when required for use.
- 4 Senior House Staff will keep a record of pupils' mobile phone numbers.
- 5 Mobile phones (incorporating cameras) that transmit images may not be used in such a way as to compromise the safety of others.
- 6 Any unacceptable use of the internet via personal mobile phones will be dealt with in accordance with the School's Behaviour and Discipline Policy.
- 7 In emergencies, pupils may request to use the School phone. Parents wishing to contact their children in an emergency should always telephone the School office and a message will be relayed promptly.
- 8 Pupils may not bring mobile phones into examination rooms under any circumstances.
- 9 The School does not accept any responsibility for the theft, loss of, or damage to, mobile phones brought onto School premises.
- 10 The School reserves the right to confiscate a pupil's mobile phone for a specified period of time if the pupil is found to be in breach of this protocol. The pupil may also be prevented from bringing a mobile phone into the School temporarily or permanently and at the sole discretion of the Head.

Appendix 3

[Pupils' handbook]

Camera, photograph and video protocol

- 1 Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.
- 2 Pupils are not allowed to operate mobile phones at all during school hours. They may only use cameras or phones or other devices with the capability for recording and/or storing still or moving images with the express permission of the member of staff in charge and with the permission of those appearing in the image.
- 3 All pupils must allow staff access to images stored on mobile phones and/or cameras and must delete images if requested to do so.
- 4 Posting of photographic material which in the reasonable opinion of the School is considered to be offensive on web sites such as Youtube, Facebook etc is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material. This is the position whether the computer used is a school computer or a computer operated elsewhere including the pupil's home.
- 5 If the School has reasonable grounds to believe that a pupil's mobile phone, camera or personal laptop computer contains images, text messages or other material that may constitute evidence of criminal activity he / she may hand the phone, camera or laptop to the police for examination.
- 6 Use of cameras, mobile phones with camera facilities or laptop computers in breach of this policy may result in confiscation of the equipment until the end of term and the pupil may be permanently banned from bringing a camera, mobile phone or laptop onto school premises in future.

Appendix 4

[Pupils' handbook]

Other electronic equipment protocol

- 1 Personal music players such as MP3 players, handheld game consoles (such as PSPs), laptops and other electronic equipment should not be brought into School without consent from a member of staff.
- 2 If such items are brought into School they may be confiscated.

Appendix 5

[Pupils' handbook]

Mobile phones protocol for communication between staff and pupils

- 1 The Royal Hospital School is committed to safeguarding and promoting the welfare of children at the school. As part of our safeguarding policy we expect staff and pupils, and where appropriate, parents, to follow this protocol on communication by mobile phone. Throughout this protocol the term mobile phone includes a PDA or similar device.

On School premises

- 2 Staff and pupils should avoid using mobile phones to speak to or send each other messages whilst in school. Phone numbers should not be exchanged or displayed. Any messages that are sent should be brief and courteous.

Emergencies

- 3 Staff on supervisory duties in the play ground, on playing fields or in relation to transport may carry and use a mobile phone to seek assistance from colleagues or emergency services.
- 4 Where a pupil or group of pupils are involved in an emergency situation they may use a mobile phone to seek assistance.

Outside School

- 5 Again, staff and pupils should avoid using mobile phones to speak to or send each other messages outside school. Any messages that are sent should be brief and courteous.
- 6 The leader of an educational visit will carry a mobile phone supplied by the school and, as part of the preparations for the visit, will ensure that other adults taking part in the visit are equipped with mobile phones and that relevant numbers are exchanged.
- 7 Staff and pupils taking part in such visits should avoid using mobile phones to speak or send messages to each other except in emergencies. Any messages that are sent should be brief and courteous.

Inappropriate communications

- 8 If there are reasonable grounds to believe that inappropriate communications have taken place, the Head will require the relevant mobile phones to be produced for examination. The usual disciplinary procedures will apply. Pupils may expect to have mobile phones confiscated if there has been a breach of this protocol.