ROEDEAN MOIRA HOUSE
ICT ACCEPTABLE USE 2018-19

This policy is for the whole school including the Early Years Foundation Stage (EYFS).

Aim

This policy applies to all staff and pupils who use the school's ICT facilities, whether this be on-site or externally and sets down the standards which users are required to observe to ensure safe and effective use. Pupils, parents and staff should read the policy carefully, making sure that the conditions for using ICT at Roedean Moira House are understood and agreed.

Security

- You may only log on with your own username and password to gain access to the school network. Passwords must be kept confidential. Passwords should not be shared. You are accountable for all actions which take place under your username. If you suspect that someone else knows your password you are responsible for ensuring it is changed at once.
- Computers must never be left unattended whilst logged in. You must either log off or lock the computer screen.
- The installing or uninstalling of non-approved software on any school computer is not permitted.
- Attempting to bypass security restrictions is strictly forbidden. Any person or student who attempts to disable, defeat or circumvent any of the school's security systems will be subject to disciplinary action.
- Virus alerts must not be ignored and must be reported to the IT department immediately.

General Internet Use

- Access to the Internet is a privilege, not a right and that access requires responsibility by all users.
- You must conduct yourself honestly and appropriately on the internet and respect the copyrights, software licensing rules, property rights, data protection guidelines, privacy and prerogatives of others.
- You must be especially careful not to disclose any personal or identifying details when using Web 2.0 technologies such as social networking sites, video sharing sites, blogs and chat rooms. Under no circumstances should personal or school details e.g. names, photographs, telephone numbers and addresses be displayed or given out. If you are uncertain of this guidance please take advice form a senior member of staff or a member of the IT Department.
- You may only download software for direct business or academic use and must arrange to have such software properly licensed and registered where required.
- Downloaded software must only be used under the terms of its license. The IT department must be consulted before any software is installed.
- Under no circumstances should you upload videos to video sharing sites, such as YouTube, that identify Roedean Moira House or any member of the school community without first gaining permission from the Principal.
- The use of Peer-2-Peer (P2P) file sharing programs, e.g. BitComet and Bearshare are strictly forbidden on any computer connected to the school's network. This includes pupils' own laptops when connected to the school's wireless network.
- You will not intentionally visit sites that attempt to bypass the school's Internet filtering and security systems.
- Under no circumstances should you view, upload or download any material which is likely to be unsuitable for children. This applies to any material with violent, dangerous, offensive or inappropriate content including images of a sexual nature. If pupils are unsure they need to

ask their personal tutor. If pupils accidentally access inappropriate material they should inform their personal tutor and/or the IT department immediately.
- You will not use the Internet, including messaging systems or chat rooms, either in school or through private access, to make defamatory or insulting comments or post images about any person.

Social Networking

Social networking sites such as Twitter, Facebook and Flickr allow users to be incredibly creative, keep in touch with their friends and express themselves using a whole range of different media and applications such as video, photos, music and chat. While social networking has many positive uses, it is important to recognise that there are also potential risks including cyberbullying, contact by adults with a sexual interest in children and the misuse of personal information. You can avoid these risks and enjoy social networking sites by following a few sensible guidelines:

- You must keep your passwords private.
- You should change the default security settings to "private" to ensure only people known to you can view your profile.
- You should select a suitable profile photo. Photos can easily be copied, changed and shared and can potentially stay online forever. Ask yourself "would you want a future employer to see this photo?"
- You should think before you post. What starts as a joke or gossip can quickly escalate to cause real pain or even break the law.
- You must be extremely careful not to give out personal information, such as email addresses, phone numbers or home addresses. Recipients of your personal information may not always be trustworthy and honest.
- If you are a student, meeting someone you have only been in touch with online can be dangerous. You must only do so with your parents' permission and even then only when they can be present.
- You should be careful before accepting emails, IM messages, or opening files, pictures or texts from people you do not know or trust as they may contain viruses or nasty messages.
- You should be aware that information you find on the Internet may not be true, or someone online may be lying about who they are.
- If you are a student, you must tell your parent or a trusted adult if a social networking contact makes you feel uncomfortable or worried.

Monitoring Internet use

- Internet access is available to all staff and students with access to a computer which is connected to the School's network. The School has a security system in place that monitors, records and filters all Internet activity. This includes traffic to/from students' own laptops connected to the school's wireless network.
- Smoothwall provides access to web pages on the Internet by use of a categorisation system. Every web page is categorised according to its content, and facilities exist to block access to certain categories; for example access is blocked to sites categorised as pornography, gambling, criminal content etc.
- It is acknowledged that certain staff and students may require, during the normal course of their duties, access to certain sites that may normally be blocked. It is possible to make exceptions in these cases to allow legitimate access, by contacting the IT department.
- Internet access is extended after (and before) School hours, in that the category restrictions are relaxed. For example access to social networking, games and video sites are allowed.

Email

Staff and pupils need to be aware that email carries exactly the same status as other forms of communication, including letters, memos and telephone conversations, and the same consideration and legal implications need to be applied and observed in the use of e-mail as in these other forms of communication.

- It is not permitted for users to send sexual, racially biased or other inappropriate emails.
- Do not use aggressive, abusive or deliberately anti-social language. Never e-mail hastily or out of anger.
- You must not copy or download or forward material that is obviously libellous (or otherwise unlawful), unrelated to work, or inappropriate in any way, i.e. graphic images, sound files, or music.
- You should, where possible, avoid sending large graphics or scanned images. The size limit for an attachment is 50MB.
- Roedean Moira House monitors all incoming and outgoing emails.
- The following disclaimer is appended to all external e-mail use.

  This e-mail and any attachments are confidential and should not be used by anyone who is not the original intended recipient. If you have received this e-mail in error please delete it and inform the sender. The opinions expressed in this email are entirely personal and do not represent the policy of Moira House School.
  All incoming and outgoing emails are virus checked, however we cannot guarantee that this message or any attachment is virus free or has not been intercepted and amended. Moira House School accepts no liability in respect of any damage sustained as a result of receiving this message or any attachments.

- Use of email for personal reasons is permitted but must not affect your duties and responsibilities, the duties of other staff or students, disrupt the system, or harm the School's image or reputation.
- Users are reminded that they are responsible for their own email housekeeping.
- Unwanted email should be deleted or archived regularly. Individual mailboxes are limited to 100MB.

Personal Devices and other Electronic Equipment

- Personal devices should not be left unattended. When not in use they should be left in the lockers provided.
- Moira House does not accept any responsibility for the theft, loss of, or damage to, personal electronic equipment brought onto School premises.
- Moira House reserves the right to hold a pupil's personal electronic device for a specified period of time.

Camcorders /any device capable of video recording

Pupils and staff are not permitted to video or take sound recordings of any school event, activity or lesson involving any member of the school community using personal camcorders or smartphones.

Mobile Phones/Smart Phones

If you are a student, you are permitted to use mobile phones in Common Rooms and form bases only, in your free time e.g. lunch, break times and in the school minibus to and from school, and then only if their use does not impact on others. Mobile phones must always be switched off during lessons and study time and kept securely in your bag or out of sight and access; for younger students, mobile phones are kept in the Office during the day. In emergencies, pupils may request to use the School phone. Staff may grant permission for students to use their mobile telephones for educational purposes.

Pen Drives

Staff and pupils may use memory sticks however inappropriate images or text found on these flash drives will be considered a violation of this Acceptable Use Policy. Pen drives are one of the main causes of data loss. Either pen drives should not be used to hold personal information (i.e. School Reports) or they should be password protected and fully encrypted using Windows BitLocker or other encryption software. Please seek advices from the IT Department if you are unsure.

Laptops/iPads/tablets and similar devices

You are permitted to use your own laptop in school. Internet access on personal laptops must be obtained through the school network. The School takes no responsibility for the consequences of using broadband networks other than the School's own.
Any laptop/iPads/tablets and similar devices lent to you by the school are the property of Moira House Girls School and must be returned to the IT Department immediately when requested.

Webcams

Standalone webcams or integrated webcams in laptops are to be used only in communal study areas or classrooms and then only if their use does not impact on others. It is specifically prohibited to use webcams in bedrooms.

Sanctions

Failure to comply with the terms of this Acceptable Use Policy may result in disciplinary action. This can include written warnings, withdrawal of access privileges, detentions and in extreme cases, temporary exclusion or dismissal from the school.

Moira House also reserves the right to report any illegal activities to the appropriate authorities.

Related policies and documents

This policy should be read in conjunction with the following policies and documents:

Employee Handbook
Staff Handbook
Code of Conduct for Employees
Health Safety Handbook

ROEDEAN MOIRA HOUSE
ICT ACCEPTABLE USE 2018-19

Boarding Staff Handbook
National Minimum Standards for Boarding Schools
ISI Handbook for the Inspection of Schools, Regulatory Requirements
Teachers' Standards
Departmental Handbook
Keeping Children Safe in Education
Safeguarding Policy
Complaints Policy (Parents)
Complaints Policy (Pupils)

POLICY REVIEWED BY SCHOOL: May 2018

POLICY REVIEWED BY SCHOOL COUNCIL:

NEXT REVIEW: May 2019