Eggar's School

Student Acceptable Use Policy

Reviewer	ICT Systems Manger
Reviewed	June 2023
Next Review Date	June 2025

London Road | Holybourne | Alton | GU34 4EQ
T: 01420 541194 | W: www.eggars.net | E: enquiries@eggars.hants.sch.uk

A. VISION

1. The school has provided computers for use by students as an important tool for learning. Use of school computers, by students, is always governed by the following policy. Please ensure you understand your responsibilities under this policy and direct any questions or concerns to the Network Manager in the first instance.
2. All users of the network have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. The school recognises and understands the link between unhealthy use of IT and in particular social networking on poor mental health. Systems and processes are in place to monitor social network use in school, and the curriculum teaches students about appropriate use of this technology.
3. Please note that use of the school network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the school, staff and students, to safeguard the reputation of the school, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

B. AIM

1. To develop the integration of the Internet and e-mail use, along with other forms of computer technology, into classroom programmes across the curriculum.
2. To develop the abilities of students to select Internet sources appropriate to their needs.
3. To provide the opportunity to develop the skills and confidence to use Internet and e-mail effectively and efficiently.
4. To encourage the use of multimedia equipment e.g., digital cameras, camcorders and projectors and interactive boards.
5. To encourage students to find specific information on the Internet, in conjunction with other forms of information technology.

C. MEANS (CLASSROOM APPLICATION)

1. Students are not to use the Internet or e-mail unsupervised.
2. No user may deliberately or carelessly waste computer resources or disadvantage other users.

D. RESPONSIBILITIES

1. Consideration must be given to avoiding inconvenience to other computer users.
2. Always log off your machine before leaving.
3. Leave computer ready for the next user to log on.
4. Do not leave programs running on computers when you leave.
5. Return furniture to normal position when you leave.
6. Report any problems to a member of staff or IT Support.

E. MONITORING

1. Records kept on all users' computer accounts (including any e-mails sent or received) are automatically the property of Eggar's School. Due to this, these materials may be subject to monitoring.
2. From time to time, the contents and usage of e-mail may be examined by the school or by a third party on the school's behalf. These included electronic communications, which are sent to you or by you, both internally and externally.
3. All messages of the school's system will be treated as education or business-related messages, which are monitored. Accordingly, students should not expect that information or documents transmitted or stored on the Eggar's School network would be private.
4. All students are to be aware that the school can monitor use of the Internet on the network, both during working hours and outside of these hours. This includes the sites and content that you visit and the length of time you spend using the Internet.
5. Inappropriate use of e-mail or Internet facilities for personal reasons during school hours may lead to appropriate sanctions.
6. Eggar's School have hardware and software in place to monitor all activity on school computers. Any inappropriate use will be captured and stored permanently for your safety and protection. This system also helps prevents any parts of this policy being broken.

F. CONTENT

1. E-mail correspondence should be treated in the same way as any other correspondence, such as a letter or a fax. That is, as a permanent written record that may be read by persons other than the addressee and which could result in personal or the school's liability.
2. Students and/or Eggar's School may be liable for what is said in an e-mail message created by a student. E-mail is neither private nor secret. It may be easily copied, forwarded, saved, intercepted and/or archived and may be subject to discovery in litigation. The audience of an inappropriate comment in an e-mail may be unexpected and extremely widespread.
3. E-mail content that may seem harmless to one person may in fact be highly offensive to another. All users need to be aware therefore, of acceptable and unacceptable use, which is detailed further in the policy. Also, all users need to be aware that unacceptable e-mail use will prompt the school to consider the response and sensitivities of the recipient's e-mail rather than the intention of the sender.
4. If anyone receives inappropriate material by e-mail, it should be reported to their teacher or to the ICT Systems Manager and not forwarded to anyone else. It is appropriate to discourage the sender of the inappropriate material from sending further materials of that nature.

G. CHAT/INSTANT MESSAGING

1. Real time chat is not to be used by students unless instructed by a teacher for educational purposes.

2. Content within IM's are to be considered under the same circumstances as e-mails. Anything typed into an instant message is therefore subject to the same conditions under this policy as e-mail is.

H. DISTRIBUTION AND COPYRIGHT:

1. Copying of any copyrighted software from any computer on the school's network is not allowed.

I. PRIVACY

1. Students will be assigned a login name and will also be required to select a password to use the Eggar's School computer network. It must be ensured that these details are not disclosed to anyone.
2. It is recommended that students change their password regularly and that staff members ensure that their login code and password are not kept in writing close to their working area.
3. Students must not disclose passwords to anyone, must not use any passwords other than their own, must not read other people's e-mail and must not reveal personal information.

J. ENCRYPTION AND CONFIDENTIALITY

1. Internet and e-mail are an insecure means of transmitting information. Therefore, items of a highly confidential or sensitive nature should not be sent by e-mail. It should be noted that there is always a trail and a copy of an e-mail saved somewhere, not necessarily on the school's server.
2. All e-mails sent from students that leave the school will contain this disclaimer message – The contents of this email are confidential. Any unauthorised use of its contents is expressly prohibited. If you have received this email in error, please advise enquires@eggars.hants.sch.uk and then delete all electronic and hard copies.
3. The e-mail disclaimer message is set to appear automatically on all outgoing e-mail. IT support is to be contacted if this feature is not working.
4. There is a risk of false attribution of e-mail. Software is widely available by which e-mail messages may be edited or 'doctored' to reflect an erroneous message or sender name. The recipient may therefore be unaware that he or she is communicating with an impostor. Accordingly, staff members should maintain a reasonable degree of caution regarding the identity of incoming mail. Verification of the identity of the sender by other means must be made if staff members have concerns.
5. Old unnecessary e-mail messages are to be deleted and only those e-mail messages that need to be kept are to be archived. Retention of messages fills up large amounts of storage space on the network server and can slow down performance. Staff members should maintain as few messages as possible.
6. You must ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.

K. VIRUSES

1. All external files and attachments must be virus checked using scanning software before they are accessed. The Internet is a potential host for computer viruses. The downloading of infected information from the Internet is potentially fatal to the Eggar's School computer network.
2. "Don't click on what you don't know" – avoid opening e-mails with attachments from people you do not know. A document attached to an incoming e-mail may have an embedded virus.
3. Virus checking is done automatically through Anti-Virus software installed on school computers. Students concerned with any e-mail attachments, or they believe that attachments have not been scanned for viruses, should contact IT support and the ICT Systems Manager.

L. BYOD (Bring Your Own Device)

1. Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff and must not be used until approved. This test must be performed at regular intervals as required by school's normal rules on electrical safety testing.
2. You must not connect personal computer equipment to school computer equipment without prior approval from the ICT Systems Manager, apart from storage devices such as USB memory sticks.
3. Internet is decrypted and monitored on BYOD devices whilst in school.
4. Students have sole responsibility for the safety of their BYOD device.
5. Only students who have been issued with a BYOD permission card are allowed to bring a device in to school.
6. Students are only authorised to use school provided Wi-Fi.

M.ACCEPTABLE AND UNACCEPTABLE USE:

At school, electronic communications must not to be used for identified unlawful behaviour. Identified unlawful behaviour is defined by the ICT Systems Manager and defined in the school policies document as:

1. Defamation of an organisation or a person(s) within an e-mail.
2. The sending of e-mails that contain statements about or based on race, nationality, religion and/or colour of a person that is likely to insult or offend.
3. Displaying sexually offensive material that has been downloaded from the Internet.
4. Sending or receiving obscene or pornographic material.
5. Infringe copyright laws.
6. The sending of e-mails that contain statements that may be seen and interpreted as sexual harassment or sexual discrimination.
7. Hacking
8. Cloning/impersonating others.
9. Harassment of other people.
10. Deliberate creation and distribution of viruses with malicious intent.

N. Use of Social Networking websites and online forums

1. Students must take care when using social networking websites such as Facebook or Twitter, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.
   Students
   In particular:
2. Students should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm the reputation of the school.
3. Unless authorised to do so, you must not post content on websites that may appear as if you are speaking for the school.
4. You should not post any material online that can be clearly linked to the school that may damage the school's reputation.
5. You must avoid posting any material that could potentially be used to embarrass, harass, or defame the school, students or any employee.
6. You must not use Social Networking sites in school.

O. Acceptable use could include:

1. Facilitating, disseminating and gathering information.
2. Collaborative projects.
3. Resource sharing.
4. Assisting technology transfer.
5. Fostering innovation.
6. Building broader infrastructure in support of education and research.
7. Fostering professional development.
8. Assisting others (teachers and students) in learning computer skills.

P. Unacceptable use would include:

1. Accessing networks without proper authorisation.
2. Transmitting or deliberately accessing and /or receiving material that may be considered inappropriate, including threatening, sexually explicit or harassing materials, offensive or discriminatory materials, or material that may be harmful either physically or emotionally including harassment or bullying of work colleagues outside the school.
3. Communicating information concerning any password, identifying code or other confidential information.
4. Distributing and / or executing malicious scripts (Python or other)
5. Distributing and / or executing games (Flash based or otherwise)
6. Interfering or disrupting network users, services or equipment. Disruptions include but are not limited to, distribution of unsolicited advertising, propagation of viruses, in any form, and using the network to make unauthorised entry to any other machine accessible via the school's network.

7. Undertaking activities which breach Government legislation.
8. Excessive use of e-mail or Internet facilities during working hours.
9. Injuring the reputation of Eggar's School or in a manner that may cause embarrassment to Eggar's School and/or the school's administration.
10. Sending 'spam' (unsolicited advertising focused e-mail) or mass mail.
11. Sending or receiving chain mail.
12. Infringing on the copyright or other intellectual property rights of another person.
13. Accessing websites that contain information on making or using weapons, booby traps, dangerous practical jokes or 'revenge' methods.
14. Unacceptable use may represent misconduct and/or serious misconduct and could result in disciplinary action, including termination of an employee's employment or contractor's engagement.
15. Unacceptable use by students will result in restriction of their computer and Internet privileges. Students may also face detention or other disciplinaries because of such actions. The school will explicitly notify parents about any unacceptable use by their child/children.
16. Students must accept the Eggar's School Acceptable ICT Use Agreement before they login to the school's network. Parents will be advised to read the schools Acceptable ICT Use Policy. If there are any queries regarding the policy, they can contact the school on enquiries@eggars.hants.sch.uk or by calling the school's office.

Q. Students must not:

1. Do anything likely to cause damage to any equipment, whether deliberately or carelessly.
2. Steal equipment.
3. Vandalise equipment (e.g., graffiti).
4. Mark or deface any equipment.
5. Interfere with networking equipment such as hubs and cables.
6. Eat or drink near any school-owned computer resource.
7. Use services or software to bypass any security or filter put in place on the school's network.

R. Students must not without permission:

1. Attempt to repair equipment.
2. Unplug cables or equipment.
3. Move equipment to another place.
4. Remove any covers or panels.
5. Disassemble any equipment.
6. Disable the operation of any equipment.
7. Students are not to bring or download unauthorised games to school.

S. Websites

1. Eggar's School have a modern, well known internet filtering service. This service helps prevent inappropriate websites being viewed by all users of the network. Its primary role is to safeguard our students and staff.

2. Use of proxy bypasses (especially VPN's) are prohibited and is a serious offence.

T. Reporting Problems with the Computer System

1. You should report any problems that need attention to a member of IT support staff as soon as is feasible.
2. If you suspect your computer has been affected by a virus or other malware, you must report this to a member of IT Support staff immediately.
3. If you have lost documents or files, you must report this as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable (mere minutes can count).

U. Backup Procedures:

1. You must make your own backup of data kept on any storage system for disaster recovery purposes. This includes USB memory sticks (even those owned or issued by the school) or a personal device. The school takes daily backups of network data. However, it is always advised to keep you own copy of important documents where possible.

V. Contacts and Links

1. These details are in the document to detail what these resources are and are of a trusted nature.
   Contacts are for information only please contact the school office directly if you wish to contact a member of staff.

2. www.eggars.net	School Website
Head Teacher	Mr Patrick Sullivan
3. ICT Systems Manager	Mr D Reseigh
4. 01420 541194	Main School Number
5. enquries@eggars.hants.sch.uk	Main School e-mail address