Greek School of Potters Bar
Greek Language Educational Establishment of Hertfordshire (GLEE)

C/O Oakmere School
Chace Avenue
Potters Bar
Hertfordshire
EN6 5NP

Telephone
07790 868 075

Email
info@greekschoolpottersbar.org

GLEE is a Registered Charity
Charity No. 1040670

Internet Acceptance Use and Data Security Policy 2018

(This document complements the School's IT Acceptable Use Policy, eSafety Policy)

Table of Contents

1 Introduction
1.1 Monitoring
1.2 Breaches
2 Whole-school Network Security Strategies
2.1 Hardware and software infrastructures
2.2 Classroom management structures
2.3 Equal Opportunities
3 Risk Assessment and Management of Internet Content
4 Regulation and Guidelines
4.1 E-mail
4.2 E-mailing Personal, Sensitive, Confidential or Classified Information
4.3 The School's website
4.4 Social networking sites, blogs and chat rooms
4.5 Other communication technologies (see also mobile phones and portable electronics policy)
4.6 Computer Viruses
5 Data Security
5.1 Security
6 Communicating the School's AUP
6.1 Informing students
6.2 Informing staff
6.3 Informing parents / carers
7 Responsibility

1.0 Introduction

The Internet, in many guises, offers extensive potential to our educational endeavours. The Governing Body endorses and encourages the widespread use of Information Technology in learning and teaching. The main reason that the School provides Internet access to our staff and students is to promote educational excellence by facilitating resource sharing, innovation, and communication. However, for both students and staff, Internet access at school is a privilege and not an entitlement. The Governing Body will not object to the reasonable use of IT systems for personal activities or recreational purposes. It must be for staff to use their common sense as to what is reasonable and if they are in any doubt to seek guidance from the Head Teacher. Activities such as gaming or online gambling are considered inappropriate and as such could lead to disciplinary action. Unfortunately there is the possibility that students will encounter inappropriate material on the Internet. The School will actively take all reasonable precautions to restrict student access to both undesirable and illegal material. Teaching staff are responsible for guiding students in their on-line activities, by providing clear objectives for Internet use. Teaching staff will also ensure that students are aware of what is regarded as acceptable and responsible use of the Internet. The main goal is to utilise Internet access to enrich and extend those learning activities that reflect the curriculum requirements and the age and maturity of the students.

1.1 Monitoring

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees, members or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2000, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

1.2 Breaches

A breach or suspected breach of policy by a School employee, member, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

2 Whole-school Network Security Strategies

The School's computer network security systems are reviewed regularly. All access to the School network requires entry of a recognised username and password. Staff, members and students must log out after every network session and must not disclose these details to anyone, nor try to use any other person's username/password. No user must access, copy, remove or otherwise alter any other user's files, without their express permission.

The School may monitor usage of IT systems, email and other digital communications to ensure they are being used in a responsible manner, to ensure there is no risk to users' safety or to the safety and security of the IT systems.

The School has the responsibility to provide safe and secure access to technologies. When using personal handheld/external devices (including PDAs, laptops, mobile phones, USB devices) in school, users will follow the

rules set out in this policy, as well as any additional rules set by the School about such use. Any such devices must be protected by up-to-date anti-virus software and free from viruses.

2.1 Hardware and software infrastructures

The School uses the following strategies to reduce risks associated with the Internet:

- Proxy server – in conjunction with a web management system
- Client Server network – in conjunction with an information and web management system
- Filtering software
- Firewall

The School uses virus protection which is updated regularly. However, files downloaded (e.g. images or software) from the Internet - or the opening of email attachments - from anywhere other than well-trusted sources can be a cause of virus infection. Infection of the School's IT systems, either intentionally, or through neglect of reasonable care could lead to disciplinary action.

The School uses software which actively monitors user input and flags any inappropriate content regardless of what software staff and students are using. This is monitored by ICT authorised staff and violations are forwarded to appropriate Governing Body members.

2.2 Classroom management structures

Computers are positioned in such a way that monitors are easily observed by teaching staff or monitored via classroom control software.

2.3 Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

3 Risk Assessment and Management of Internet Content

All students are taught effective online research techniques. These include:

- Ensuring the validity, currency and origins of the information accessed or received;
- Using alternative sources of information for comparison purposes;
- Identifying an author's name, date of revision of the materials, and
- possible other links to the site;
- Respecting copyright and intellectual property rights.

When using the internet in a professional, educational or school sanctioned personal capacity, permission must be obtained to use the original work of others. Copyrighted, material must not be copied, downloaded or distributed. In conjunction with the data protection policy, staff, member and student data will be kept private and confidential, except where it is required by law or by school policy to disclose such information to an appropriate authority.

Staff and students will be made aware of the risks to which they may be exposed while on the Internet. They will be shown how to recognise and avoid the negative areas of the Internet such as pornography, violence, racism,

extremism and exploitation of children. However, if they encounter such material they will know that they should report the incident to the nearest teacher or a member of the Governing Body who will deal with it according to the School Internet Acceptance Usage Policy. Materials which are illegal, inappropriate or which may cause distress to others must not be uploaded, downloaded or accessed.

4 Regulation and Guidelines

The School's Internet access incorporates a filtering system, as well as pre-filtered content via Hertfordshire County Council provision to block inappropriate websites. The filtering system used on the School network aims to achieve the following:

- Block access to inappropriate sites
- Dynamically filter the content of web pages or web searches for unsuitable words.
- A rating system is used to rate web pages for inappropriate content and that the web browsers are set to reject these pages.

The Oakmere School's Network Manager regularly assesses the effectiveness of the filtering system. The School will immediately report the details of any inappropriate or illegal Internet material found to Oakmere School's Network Manager.

4.1 E-mail

The school gives the governing body access to the school's central email account to use for all school business as a work based tool. This is to protect members, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

- Under no circumstances should members contact pupils, parents or conduct any school business using personal email addresses;
- Members and staff sending e-mails to external organisations, parents or pupils must be checked carefully before sending, in the same way as a letter written on school headed paper. Members and staff are advised to cc. the Head Teacher, Chairman or designated accountable person where appropriate.

The School may use an e-mail distribution list to send messages to selected groups of users, with appropriate permissions to stop students sending emails to groups. This can be achieved and is not limited to the use of the BCC method in the email.

Students should not reveal their own or other people's personal details, such as addresses or telephone numbers or arrange to meet someone outside school via any School network.

Users should not open any attachments to e-mails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs.

E-mail must not be used to propagate offensive or inappropriate material in any way, even if such material was not sourced from the School's systems. This includes 'spam' messages whereby multiple unsolicited messages or unwanted material are sent in an effort to congest a recipient's mailbox or to harass or stalk the recipient. Students should immediately report any offensive e-mails that they receive to a member of staff or Governing Body member.

E-mails created or received as part of your School role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account.

4.2 e-mailing Personal, Sensitive, Confidential or Classified Information

Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible.

- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted
- Where your conclusion is that e-mail must be used to transmit such data:
- Obtain express consent from the Chairman or Head Teacher to provide the information by e-mail;
- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
  - Verify the details, including accurate e-mail address, of any intended recipient of the information;
  - Verify (by phoning) the details of a requestor before responding to e-mail requests for information;
  - Do not copy or forward the e-mail to any more recipients than is absolutely necessary;
  - Do not send the information to any person whose details you have been unable to separately verify (usually by phone);
  - Send the information as an encrypted document attached to an e-mail;
  - Provide the encryption key or password by a separate contact with the recipient(s);
  - Do not identify such information in the subject line of any e-mail;
  - Request confirmation of safe receipt.

In exceptional circumstances, the Hertfordshire County Council makes provision for secure data transfers to specific external agencies when using the Oakmere School's network. Such arrangements are currently in place with:

- Hertfordshire Constabulary
- Hertfordshire Partnership Trust

4.3 The School's website

All content on the website is copyright of the School. It must not be copied or reproduced without express permission in writing from The Chairman. The School is not responsible for content of external websites, even if links are provided to those sites.

The School will not associate a photograph of a pupil with their name. Students' names may be published on the site and the School may publish photographs containing their image, but it will never be possible to identify a child's name from the photograph without the express permission of the parent/carer being sought.

4.4 Social networking sites, blogs and chat rooms

Use of external resources (such as blogs and social networking sites) must be undertaken with planning and care with regard to the age of students and the suitability of the site, to ensure that the privacy of students is not compromised, and that students are not exposed to bullying. It is also the responsibility of the teacher to moderate material placed online if the facility is provided as a school resource. If the teacher is in any doubt as to the appropriateness of such use they should consult The Head Teacher in the first instance and/or a member of the Governing body.

4.5 Other communication technologies (see also mobile phones and portable electronics policy)

Students are not allowed to use mobile devices during lessons or formal school time, unless given express permission from a member of staff. The use of any personal handheld/external devices (whether for music, data storage, or communication) is at the discretion of the teacher in charge. It is forbidden to send abusive or otherwise inappropriate text messages. Personal equipment should not be used to record sound or images unless

prior permission has been given. Staff must not engage in any online activity that may compromise their professional responsibilities.
For their own protection, staff and members of the Governing Body should only communicate with students and parents/carers using school systems. Use of personal communication systems could be misconstrued.

4.6 Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media must be checked for any viruses using appropriate anti-virus software before using them.
Never interfere with any anti-virus software installed on school ICT equipment that you use.
If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact a member of the Governing Body immediately. The Governing Body will advise you what actions to take and be responsible for advising others that need to know.

5 Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.
The guidance documents are listed below:

- Head Teacher's Guidance – Data Security in Schools – Dos and Don'ts
- Network Manager/MIS Administrator – Data Security in Schools
- Staff Guidance – Data Security in Schools – Dos and Don'ts
- Data Security in Schools - Dos and Don'ts

The Head Teacher, Chairman of the Governing Body and Secretary documents contain advice about identifying information assets including a brief outline of the school policy that can be displayed at appropriate sites within the school or handed to visitors or guests.

5.1 Security

The School gives relevant staff access to its Management Information System, with a unique ID and password. It is the responsibility of everyone to keep passwords secure.
Staff are aware of their responsibility when accessing school data and have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use.
Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.
Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under their control at all times.
It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared printers (multi-function print, fax, scan and copiers) are used.

5.2 Disposal of Redundant ICT Equipment

All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
Disposal of any ICT equipment will conform to:

- The Waste Electrical and Electronic Equipment Regulations 2006
- The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

- Data Protection Act 2000
- Electricity at Work Regulations 1989

6 Communicating the School's Acceptable User Policy

6.1 Informing students

ICT and online resources are increasingly used across the curriculum. The School believes that it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within the curriculum and staff continually look for new opportunities to promote eSafety.

Students will be informed that their Internet use is monitored and be instructed on safe and responsible use of the Internet.

6.2 Informing staff

All staff will be provided with a copy of the School's Acceptable Use Policy. Staff are aware that Internet traffic can be monitored and traced to an individual user. Staff will be consulted regularly about the development of the School's Acceptable Use Policy and instructions on safe and responsible Internet use. To avoid misunderstandings staff should contact the Network Manager if they are in any doubt about the legitimacy of any use of the internet. Teaching staff will be provided with information on 'copyright and the Internet' issues that apply to schools.

6.3 Informing parents / carers

Parents' attention will be drawn to the School Acceptable Use Policy in the School newsletter and on the School's website. Advice that accords with acceptable and responsible Internet use by students at home will be made available to parents.

7 Responsibility

All users are responsible for their actions both in and out of school. This internet acceptable use policy applies not only to work and use of school IT equipment in school, but also applies to the use of school IT systems and equipment out of school, and the use of personal equipment in school or in situations related to the School. Failure to comply with this acceptable use policy could be subject to disciplinary action.

Issued and approved by:

…… Mr Andrew Pantelli (Chairman)

…….. Mrs Stella Nadiotis (Head teacher)