Acceptable Use Policy

Ermysted's Grammar School

The Governing Body of Ermysted's Grammar School (the 'School') ratified this policy on 23 August 2023.

Introduction

The intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to the School's established culture of openness, trust and integrity. The School seeks to protect its staff, pupils, and the Governing Body from illegal or damaging actions by individuals, either knowingly or unknowingly. It is the responsibility of every school computer user to be familiar with these guidelines and to conduct their activities accordingly.

This Acceptable Use Policy outlines the guidelines and behaviours that all users are expected to follow when using school technologies or personally-owned devices on the school site.

- The school network is intended for educational purposes
- All activity over the school network may be monitored and records retained
- Access to online content via the network may be restricted in accordance with school and national policies and guidelines
- Members of staff and pupils are expected to follow the same rules of behaviour and conduct online as offline
- Misuse of school resources can result in disciplinary action
- Ermysted's makes a reasonable effort to ensure the safety and security of staff and pupils online and will not be held accountable for any harm or damages that result from misuse of school technologies
- Users of the Ermysted's network are expected to alert IT staff immediately of any concerns for safety or security

Technologies Covered

Ermysted's may provide internet access, desktop computers, mobile computers or devices, online collaboration capabilities, message boards, email, and more. As new technologies emerge, the School will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

Usage Policies

All technologies provided by the School are intended for educational purposes. All users are expected to use good judgment and to follow the specifics of this document: be safe, appropriate and courteous.

Web Access

The School provides users of its network with access to the internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with school and national policies. Users are expected to respect that the web filter is a safety precaution and should not try to circumvent it when browsing. If a site is blocked and a user believes it should not be, the user should ask for the block to be reviewed.

Email

The School provides members of staff and pupils with email accounts. Only school accounts should be used for school-related communication. Users should not attempt to open files or follow links from unknown or untrusted sources. They should use appropriate language and should communicate with other people only as

guided by school policy using these accounts. The school reserves the right not to recognise records of school-based communication maintained through email accounts other than the user's school account.

Social media and other collaborative content

The School may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. The guidelines for all other forms of communication, regarding confidentiality and courtesy, for example, apply here.

Mobile Devices Policy

The School may provide users with mobile devices to promote learning both inside and outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network. Users are expected to treat these devices with care and caution. Users should report any loss, damage, or malfunction to IT staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse. Use of school-issued mobile devices, including use of the school network, may be monitored.

Personally-Owned Devices

Staff and pupils are allowed to have personally-owned devices on site – including laptops/tablets (staff and sixth form only), smartphones and cell phones – but pupils must not use these in lessons without the explicit permission of the teacher.

Any inappropriate use of personally-owned devices may result in disciplinary action. Staff and pupils should not download any data from the School's systems onto private cloud-based storage, personally-owned devices or any other form of storage device such as a memory stick.

Any information or data which staff and pupils may require in the course of their work can be accessed through the school's approved remote channels. (Specific exceptions may be permitted with the explicit prior agreement of the Headteacher or School Business Leader.)

Security and Proprietary Information

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If you believe a computer or mobile device you are using might be infected with a virus, please alert a member of the IT support staff. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Authorized users are responsible for the security of their passwords and accounts. Computers should be secured with a password-protected screensaver or by logging-off when left unattended. Multi-Factor Authentication is enforced for all staff school accounts to reduce the risk of unauthorised access or hacking when using remote access.

All pupil and staff details, including photographs and other media, are considered to be confidential and should not be disclosed to third parties, without the prior agreement of the Headteacher.

Downloads

Users should not download or attempt to download or run *.exe* programs over the school network or onto school resources without express permission from the IT staff. Users should download other files only from reputable sites, and only for educational purposes. Users should not enter into any contractual agreements using school equipment.

Netiquette

Users working on behalf of the school should always use the internet, network resources, and online sites in a courteous and respectful manner. Users should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.

Plagiarism

Staff and pupils should not plagiarise content (or use as their own, without citing the original creator), including words or images, and videos from the Internet. Research conducted via the Internet should be appropriately cited, giving credit to the original author. In addition users must respect and comply with copyright and intellectual property rights.

Personal Safety

If users see a message, comment, image, or anything else online that makes them concerned for their personal safety, they should bring it to the attention of a senior member of staff immediately.

- Users should not share personal information, including phone number, address, national security number, birthday, or financial information using the school network
- Communicating over the internet brings anonymity and associated risks: personal information about themselves and others should be treated with the utmost caution

Cyberbullying

Cyberbullying will not be tolerated. Engaging in any online activities intended to harm (physically or emotionally) another person, will result in disciplinary action. In such cases, users are reminded that the school's jurisdiction extends beyond the school site and beyond the school day.

Limitation of Liability

The School will not be responsible for damage or harm to persons, files, data, or hardware. While Ermysted's employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. The School will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Examples of Acceptable Use

Users agree to:

- Use school technologies for school-related activities and research.
- Follow the same guidelines for respectful, responsible behaviour online that users are expected to follow offline.
- Treat school resources carefully and alert the relevant staff if there is any problem with their operation.
- Encourage positive, constructive discussion when using communicative or collaborative technologies.
- Alert the appropriate member of staff if users see threatening/bullying, inappropriate, or harmful content (e.g. images, messages or posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits only.
- Cite sources when using online sites and resources for research; ensure there is no copyright infringement.
- Recognize that use of school technologies is a privilege and treat it as such.
- Be careful to protect the safety of themselves and others.
- Help to protect the security of school resources.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Examples of Unacceptable Use

Users will not:

- Use school technologies in a way that could be personally or physically harmful to themselves or others, including posting personally-identifying information.
- Use school technologies for illegal activities or to pursue information on such activities.
- Use language online that would be unacceptable in the classroom.
- Access, or attempt to access, data of which the user is not an intended recipient or log into another staff or pupil account that the pupil is not expressly authorised to access.
- Download to a personal device or any other form of storage medium, which is off the school network or can be removed from the school site, any personal information concerning staff or pupils.
- Circumvent user authentication or security of any work-station or user account.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use the school technologies to actively engage in the viewing, creation or distribution of any sounds, messages or other material which are obscene, harassing, racist, inflammatory, malicious, fraudulent or libellous, and which would otherwise damage the reputation of the School.
- Attempt unauthorised copying of copyrighted material including digitization and distribution of photographs from magazines, books, videos, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the School or the end user does not have an active licence.
- Plagiarise content found online.
- Use school technologies to send spam or chain mail.
- Attempt to hack or access sites, servers, accounts, or content that isn't intended for their use.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Violations of this Acceptable Use Policy

Violations of this policy may result in disciplinary action.

I have read and understood this Acceptable Use Policy and agree to abide by it:

_____

(Name)

_____

(Signature)

_____

(Date)

Appendix A

Relevant legislation

The following are a list of Acts that apply to the use of EGS computing facilities:

- General Data Protection Regulation (GDPR) as it applies in the UK, tailored by the Data Protection Act 2018.
- Regulation of Investigatory Powers Act 2000
- Computers' Misuse Act 1990
- Protection from Harassment Act 1997
- Sex Discrimination Act 1975
- Race and Religious Hatred Act 2006
- Disability Discrimination Act 1995
- Obscene Publications Act 1959
- The Telecommunications (Lawful Business Practice)
- (Interception of Communications) Regulations 2000
- Protection of Children Act 1978
- Criminal Justice Act 1988
- Data Protection Act 1998
- The Patents Act 1977
- Copyright, Designs and Patents Act 1988
- Defamation Act 1996
- Freedom of Information Act 2000
- Sexual Offences Act 2003
- Human Rights Act 1998
- Communications Act 2003
- Malicious Communications Act 1988
- Public Order Act 1986

Appendix B

Use of Children's images[1]

Introduction

- Ermysted's Grammar School believes that the responsible use of children's images can make a valuable contribution to the life and morale of the school. The use of photographs in school publicity materials can increase pupil motivation and help parents and the local community identify and celebrate the school's achievements.
- We only use images that the Headteacher and Governing Body consider suitable and which appropriately represent the range of activities the school provides and the values it adheres to. No images will be used which could be considered to put any child at increased risk.
- Through this policy we aim to respect young people's and parents' rights of privacy and minimise the risks to which young people can be exposed through the misuse of images. The policy takes account of both data protection and child protection issues.

Data Protection

- Photographs and video images of pupils and staff are classed as personal data under the terms of the General Data Protection Regulations 2018. We will not use images of identifiable individuals for school publicity purposes without the consent of either the individual themselves or, in the case of pupils, their parent, guardian or carer. We ask parents to consent to their child's image being used for school purposes and in the media in connection with events organised by school. The consent is requested as pupils enter the school and will be current until parents request otherwise.
- All images will be used only by those who are authorised to do so.

Child Protection

- We will only use images of children in suitable dress. The Headteacher and Governing Body will decide if images of some activities – such as sports or art – are suitable without presenting risk of potential misuse.
- Any evidence of the use of inappropriate images, or the misuse of images, will be reported to the School's designated safeguarding lead, the LA, Social Care and/or the police as appropriate.
- We will never use an image of a child who is subject to a court order.

Websites

- We will adopt the same principles as outlined above when publishing images on the internet as we would for any other kind of publication or publicity material. However, the school recognises that there is no control over who may view images, and consequently a greater risk of misuse of images, via the internet. We will therefore consider the suitability of images for use on the school's website Images, and accompanying details, will only be used in line with government guidance.

Webcams and Mobile Phones

- Pupils are not encouraged to bring mobile phones into school. Should they choose to bring a phone into school they are responsible for its security and its use. Where mobile phones which can take and transmit images are being misused, they will be confiscated. Where this occurs in areas such as toilets, changing rooms or sports facilities then this misuse will be regarded as a serious breach of school discipline and dealt with accordingly and if appropriate reported to the police.

[1] The word images is used here to include photographs, webcam footage, film and video recordings.

External Photographers and Events

- If the school invites or permits an external photographer to take photographs within school, we will:
    - Provide a clear brief for the photographer about what is considered appropriate in terms of content and behaviour
    - Issue the photographer with identification which must be worn at all times
    - Not allow unsupervised access to children or one-to-one photo sessions at events
- The same conditions will apply to filming or video-recording of events.
- Photographs taken by journalists are exempt from the General Data Protection Regulations as newspapers are subject to strict guidelines governing the press. However, wherever possible and practicable, we will secure parental permission before allowing journalists to take photographs of pupils.