

# Ealing Independent College

## IT Acceptable Use and Social Media Policy (Students)



Created August 2016

Reviewed August 2022

## IT Acceptable Use Policy

**Introduction:** This policy sets out the requirements with which you must comply when using the School's e-mail and internet services. Failure to comply will constitute a disciplinary offence and will be dealt with under the School's Disciplinary Procedure.

1. **Property:** You should treat any property that belongs to the School with respect and reasonable care, any faults or breakages must be reported to the Office immediately.
2. **Viruses:** You should be aware of the potential damage that can be caused by computer viruses. You must not introduce or operation any programmes or data (including computer games) or open suspicious emails.
3. **Passwords:** Passwords protect the School's network and computer system. They should not be obvious, for example a family name or birthdays. You should not let anyone else know your password. If you believe that someone knows your password you much change it immediately. You should not attempt to gain unauthorized access to anyone else's computer or to confidential information which you are not authorised to access.
4. **Leaving workstations:** If you leave your workstation for any period of time you should take appropriate action and, in particular, you should log off and/or set your screen saver with an appropriate password.

### Online Learning

5. **Google Meet Lessons:** The usual classroom expectations and standards of behavior apply to Google Meet Lessons. Any Students being disruptive or not participating sensibly in the online lessons will be disconnected by the teacher and parents informed.

All students agree to the following rules:

- 5.1 I will read and adhere to the pupil guidance provided by my teacher
- 5.2 I will join the Google Meets Lesson at the correct time according to my timetable
- 5.3 I will be dressed appropriately in day clothes (no pyjamas, no onesies etc.)
- 5.4 I will be seated at an appropriate table or desk in a quiet room, away from noise and distractions. (no beds)
- 5.5 I will only use the messaging feature to indicate that I have a question for the teacher
- 5.6 I will be silent throughout unless given permission by the teacher
- 5.7 I understand that it is only the teacher who is allowed to mute or disconnect other users.
- 5.8 I will not invite other members to the Google Meets Lesson
- 5.9 I will follow e-safety procedures and report to or seek advice about anything I find upsetting online.

### Internet

6. **Downloading:** Downloading of any programme or file onto the School's network or local station is strictly prohibited. Downloading of work files must be through the School's email system only.
7. **Personal Use:** The School does not permit incidental, personal use of the internet. Internet access may be withdrawn without notice at the discretion of the Principal.
8. **Unsuitable Material:** Viewing, retrieving or downloading of pornographic, terrorist or extremist material, or any other material which the school believes is unsuitable at any time is strictly prohibited and constitutes gross misconduct. Internet access may be withdrawn at the discretion of the Principal.

All allegations of unsuitable use are investigated by the School. You should be aware that all devices attached to the School network School Computers/Laptops/tablets/phones are monitored for improper/illegal use by E-Safe Systems Ltd. You will be required to sign a separate document which

details the areas and types of monitoring involved. In addition, all emails using the School email ([x.y@ealingindependentcollege.com](mailto:x.y@ealingindependentcollege.com)) are monitored as are the google apps. Linked to the College network.

## E-mail

9. **Personal Use:** All emails pertaining to School must be sent/received through the School's email system – personal emails must not be used for School business. All students will be given a School email address. If the School discovers that you have breached these requirements disciplinary action may be taken.
10. **Status:** E-mails should be treated in the same way any other form of written communication. You should not include anything in an e-mail which is not appropriate to be published generally.
11. **Inappropriate Use:** Any e-mail message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation or religious belief (or otherwise contrary to our Equal Opportunities Policy), or defamatory is not permitted. Use of the e-mail system in this way constitutes gross misconduct. The School will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate e-mails. Student should also read the e-safety policy that forms part of the Schools Safeguarding Policy (available on the School's website).
12. **Legal Proceedings:** You should be aware that e-mails are disclosable as evidence in court proceedings and even if they are deleted, a copy may exist on a back-up system or other storage area.
13. **Jokes:** Trivial messages and jokes must not be sent or forwarded to the email system.
14. **Disclaimer:** All correspondence by e-mail should contain the Schools disclaimer:
  - *This e-mail and any attachments are confidential. If you receive this message in error or are not the intended recipient, you should not retain, distribute, disclose or use any of this information and you should destroy the e-mail and any attachments or copies.*
15. **Data protection disclosures:** Subject to a number of limited exceptions, potentially all information about an individual may be disclosed should that individual make a subject access request under the Data Protection Act 1998. There is no exemption for embarrassing information (for example, an exchange of emails containing gossip about the individual will usually be disclosable). **As such students must be aware that anything they put in an email is potentially disclosable.**

## Monitoring

16. **Monitoring:** Students acknowledge and agree that the School regularly monitors and accesses the School IT system for purposes connected with the operation of the School. The School IT system includes any hardware software, email account, computer, device or telephone provided by the School or used for School business. The purposes of such monitoring and accessing include:
  - 16.1 to help the School with its day to day operations
  - 16.2 to check student's compliance with the School's policies and procedures and to help the School fulfil its legal obligations. For example, to investigate allegations that a student has been using their email account to send abusive messages or for cyber-bullying.

## Social Media Policy

**Introduction:** The School recognizes that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Instagram, Snapchat, TikTok, Twitter, and all other internet postings.

1. **Purpose:** This policy applies to the use of social media. Its purpose is to help students avoid the potential pitfalls of sharing information on such social media sites and should be read in conjunction with the e-safety part of the Safeguarding Policy (available on the School's website).
2. **IT Facilities:** This policy applies regardless of whether social media is accessed using the School's IT facilities and equipment or your personal equipment.
3. **Personal Use:** While at School, the School does not permit students to be engaged in any social media activity. Any social media activity must take place outside of School and not on School equipment.
4. **Guiding principles:** Students are required to behave responsibly at all times and adhere to the following principles:
  - 4.1 You are prohibited from accessing personal social media from School computers at any time and from a personal device whilst you are in School.
  - 4.2 You should consider carefully who you should be 'friends' with or 'followers' of.
  - 4.3 You should be mindful of how you present yourself and the School on such media.
  - 4.4 You should protect your privacy and that of others by omitting personal information from internet posts such as names, email addresses, home or work address, phone numbers or other personal information.
  - 4.5 You should familiarize yourself with the privacy settings of any social media you use and ensure that public access is restricted. If you are not clear about how to restrict access, you should regard all your information as publicly and behave accordingly.
  - 4.6 You must not post anything that may offend, insult or humiliate others, particularly on the basis of their sex, age, race, colour, national origin, religion or belief, sexual orientation, disability, marital status, pregnancy or maternity
  - 4.7 You must not post anything that could be interpreted as threatening, intimidating or abusive. Offensive posts or messages may be construed as cyber-bullying. This should be read in conjunction with the School's Anti-Bullying Policy (available on the School website).
  - 4.8 You must not post disparaging or derogatory remarks about the School or its directors, staff, staff, volunteers, pupils or parents, guardians or carers.
  - 4.9 You must not post anything that could be interpreted as glorifying or supporting terrorism, extremism or organisations promoting terrorist or extremist views, or encouraging others to do so.
5. **Monitoring:** The School regularly monitors the use of the internet, social media and email systems to check that the use is in accordance with this policy. If it is discovered that any of the systems are being abused and/or that the terms of this policy are being infringed action may be taken which could result in disciplinary action.

## **IT Acceptable Use and Social Media Policy Declaration Form (Students/Parents)**

**Student Name:** \_\_\_\_\_ **Date of Birth:** \_\_\_\_\_

I acknowledge that I have read and understood the School's IT Acceptable Use and Social Media Policy for students and that my parents/guardians must countersign the form below.

I am aware that all devices attached to the School's network – Computers, Laptops, Tablets, and Phones will be monitored by E-Safe Systems Ltd. E-Safe will look in particular for:

- Illegal / potentially illegal activity
- Accessing pornography
- Radicalisation
- Bullying / Cyber-bullying
- Sexting / Grooming
- Inappropriate comments
- Violent and Threatening behavior
- Discrimination

I understand that the School will be informed by E-Safe of any concerns about my internet use, and that the School will take appropriate action.

I understand that I am responsible for the confidentiality of my password(s) and that I will log off at terminals after each working session. You are advised that if you lose your password, or if you feel other people know your password you should get this changed through the School office without delay).

I understand that any activity, whether at school or outside school that involves use of the School's email system, this email activity will be monitored by E-Safe Systems, Apps such as Calendar, Contacts, Photos, You Tube etc. that are linked to your School email account will also be accessible to the monitoring system employed. (any emails that involve School Business/Communications should always be sent through the School email system and not through your personal email).

Student Signature: \_\_\_\_\_ Print Name: \_\_\_\_\_ Date: \_\_\_\_\_

### **Parent declaration:**

I have read the IT Acceptable Use and Social Media Policy that accompanies this form and understand that the School is using E-Safe Systems Ltd to monitor School internet and email activity. I also understand that I will ensure, using parental controls (for under 18 students) that computers at home have restricted access. I also understand that parental controls are switched on any mobile phone my son/daughter is using.

Parent Signature: \_\_\_\_\_ Print Name: \_\_\_\_\_ Date: \_\_\_\_\_