

ICT acceptable use policy - pupils

This policy is used in conjunction with the associated policies and publications referenced at the end. Pupils must be aware of the large quantity of government legislation that forms a backdrop to this area of College life. There can be a tendency for some young people to think that use of ICT is somehow removed from real life but this is very much not the case.

ICT affords huge educational, work-related and social benefits. ICT can also lead to problems. These range from spending too much time online (which can lead to underperformance in studies, lack of sleep, an inability to make genuine friendships and to take advantage of a full and productive College education), to much more serious situations where a pupil can break the law with potentially lifelong consequences.

All pupils are required to sign a copy of this AUP on arrival at the College as part of their pupil induction (which will cover instruction on how to use email, make helpdesk requests, access programmes and software and use key applications such as for sports). **A copy of the signed AUP will be held on file.**

The College provides ICT facilities and encourages the use of technology for the educational benefit of pupils. It also takes its responsibility to provide safeguards against risk, unacceptable material and activities very seriously. The use of ICT facilities, including access to email and the internet, is a privilege to pupils and not a right. The College aims to ensure that the whole community works to ensuring responsible digital citizenship.

The College has made substantial investment in its ICT provision. It is the duty of everyone in the College community to protect computer hardware, software, data and documentation from misuse, theft, unauthorised access and environmental hazards. Inappropriate use of technology may result in the removal of these privileges and / or disciplinary action.

As a part of the College community, all are expected to adhere to acceptable and responsible use of ICT whether using College facilities, their own or that of others. The College has a responsibility to ensure all pupils behave acceptably and within the letter of the law when online, whether they are on the College site or elsewhere. From a pastoral, educative and disciplinary perspective, both the tone and content of the policy is applicable and relevant to all pupils regarding the use of ICT generally throughout their time at College, whether using their own devices and ICT systems or using the College's network, hardware and ICT systems. The policy's application also transcends the term-time holiday divide.

When using the College network, Eastbourne College reserves the right to review any material on user screens and server logs to monitor file-server space, internet and email use. This enables appropriate ICT managers and / or other staff to monitor the appropriateness of work and other activity carried out on the College network. Hsms and other staff authorised by the second master, deputy head (academic) or deputy head (pastoral) may view reports to monitor individual pupil network accounts.

Filtering software is used to limit access to undesirable internet sites including those related to violent extremism. All email is scanned and actively monitored for inappropriate content. This is in order that appropriate educational and safeguarding action can be taken.

All pupils must adhere to the following rules when using the College's network services:

- Not to share your password with anyone
- To lock your workstation if you leave it temporarily
- To log off a workstation when you have finished working
- Change your password regularly, use complex passwords
- Do not open emails from unknown sources
- Do not open attachments unless the source is known. Delete them without opening
- Do not install, or attempt to install, software, applications, shareware, freeware, etc, onto the network
- Do not attempt to bypass the College's filtration and firewall systems by, for example accessing sites via a VPN (virtual private network)
- Do not trespass into other people's files, work, profiles or property
- Do not attempt to "hack" into the College systems or systems belonging to others
- You are not permitted to send global emails
- You must not attempt to access restricted sites which contravene the College rules or any sites with obscene, illegal or otherwise disturbing content. If you are unsure, imagine a parent or your hsm is viewing the site with you
- Any games or content stored, owned or used must be of the right age classification
- File storage is for academic work only, and is expected to be organised and managed appropriately
- Storage of data on USB devices is encouraged, but care is expected to be taken not to bring any harmful electronic data (eg viruses) onto the College network.

All users are expected to abide by the College values of integrity, courtesy and kindness which apply in the same way online as they do elsewhere. Expectations and understandings include, but are not limited to the following:

- Use of appropriate language. Do not swear, use vulgarities or any other inappropriate language in email or internet use
- Be polite - there should never be any abuse in your communication with others
- Under no circumstances should you reveal personal details (eg, telephone number) of yourself or any other pupil, this includes photos without prior consent
- Pupil's individual email addresses or other social media handles must never be made public
- Email is **not** private. IT managers and other authorised staff have access to all email which can be viewed at any time
- Activities which might compromise the use of the network by other users must be avoided. This includes broadcast messaging, spamming and sharing files (eg iTunes libraries)
- Any communications and information accessible from the internet should be assumed to be the property of those who posted it
- Do not request, store or send anything which is illegal. Note, **very importantly**, this includes inappropriate images of pupils, even if they are known very well to you, as they are classified as children
- Publish nothing about another person which you would not be prepared to say to their face (and thereof having to deal with the possible consequences)
- Do not post material (either by name or anonymously) about other people, especially material which is unkind, defamatory, harmful (either personally or to their work), harassing, discriminatory, illegal, inciting violence or hatred of any kind or untrue
- Do not act in a way that brings the College into disrepute.

Pupils are expected to take responsibility for management of their online presence. This includes, but is not limited to; use of social media, all forms of electronic communication and mobile devices. In their actions they should always take appropriate steps to maximise the safety, security and privacy of themselves and others in the College community. Expectations applying to this include:

- Awareness of privacy settings and adjustment of these to match individual level of comfort, with regular review
- Being cautious about posting and sharing personal information, especially information that could be used to identify you or anyone else, or locate you offline, such as your address or telephone number
- Reporting users and content that violate the Facebook (or any other social media platform) Terms of Use to your hsm and to Facebook (or alternative provider)
- Blocking and reporting anyone that sends you unwanted or inappropriate communications
- If you receive unwanted communication from a pupil at the College, report it to your hsm immediately
- You are not permitted to add members of staff as friends on social media. Please do not invite members of the teaching staff, or any College employee, to become your friend
- Being aware that content posted to the web can be copied, altered and reposted by anyone and it is very difficult to take back what may be later regretted and viewed by others
- You should always behave in a responsible manner online in the same way you would offline
- Ensuring any published work which is used in a pupil's own work is properly referenced and acknowledged (ie, not plagiarised)
- Ensuring the ownership of data and personal information is always respected and that copyright and data protection is understood and adhered to
- You will remain responsible for sending or storing any content that is inappropriate, offensive or illegal, whether it is transmitted (or stored on) from your own device, or the College's network
- If you receive any unwanted communication you must report this immediately to your hsm, deputy head (pastoral) or second master
- Telling your hsm if you encounter websites which cause you concern in any way. Our web filtration systems should evolve to protect pupils from material of an extremist / illegal, etc nature
- You must stay safe and you also have a responsibility to assist others in keeping safe. With this in mind, you should pass on concerns about other pupils' inappropriate behaviour to a member of staff. If something does not seem right, then it might well not be. For example, obsessive use of a device by a pupil could simply mean they are not getting work done or making friends. However, it could mean that they are engaged in an age-inappropriate and potentially hazardous relationship with someone whom they do not actually know
- You must not post material online which can be associated with the College name, brand or registered trademarks (including the logo, the crest, Memorial Building silhouette and the stag). If you wish for such material to use the College name, brand or trademarks, you must first seek authorisation from the director of marketing and communications via HMO in order that its content be checked
- You must not film and / or post a College / house production or activity without prior permission from both the activity organiser and the director of marketing and communications. College / house productions are generally filmed "centrally" and the footage posted to parents with access via the password protected parent portal
- You must never identify College pupils without their prior permission via online posts

- It is correct and proper to ask for someone's prior permission before posting a picture of them online, even if they are in the same photo as you.

All pupils must read and accept the College's ICT acceptable use policy before they are granted access to the network. Pupils failing to do so will not be permitted the use of electronic devices in College. A copy of the pupil declaration form can be found in Appendix I of this document.

Sanctions for improper use

Should any pupil breach the College's ICT Acceptable Use Policy, they will be dealt with in line with the disciplinary measures listed in the White Book.

Some examples (not an exhaustive list) are shown below:

Offence	Equivalent	Sanction
Cyber bullying	Bullying	Warning / SND / internal suspension / suspension / dismissal
Deliberate action undermining network security	Breaking in to a secure building	Probable suspension or permanent exclusion.
Improper use of available web sites	Misbehaviour	Red paper
Inappropriate use of email	Anti-social	E-mail account temporarily suspended / housing / gating / SND
Plagiarism	Cheating	SND
Possession / transmission of / requesting inappropriate material	Possession of unacceptable items	Housing / SND / internal suspension / suspension / dismissal NB - current advice is for all cases of sexting to involve the police - initially on an advisory basis although the consequences this potentially means for older pupils are incredibly serious
Posting online material which is associated with the College brand, name or registered trademarks, without authorisation (which may / may not additionally bring the College name into disrepute)	Publically putting / advertising a business or organisation in a bad light	Warning and material to be taken down; SND / internal suspension / suspension / dismissal
Repeated attempts to access restricted sites	Out of bounds	Warning / reflective essay writing / parents informed / gating / housing / withdrawal of ICT account
Use of age-inappropriate material	Out of bounds	Gating / housing / SND
Use of a VPN through the College internet filter	Out of bounds +	SND 1 hour / SND 2 hours / Internal suspension / withdrawal of internet access for a period / Suspension
Use of another account / password	Stealing	E-mail account temporarily suspended / SND / internal suspension / suspension
Wilful damage to equipment	Wilful damage	Charge / SND / internal suspension / suspension / dismissal

If necessary, the information systems manager may suspend the network account of any pupil while investigations are made.

It may be the case that the information systems manager / hsms / deputy head (pastoral) / second master impose further sanctions on those listed above according to the nature of the offence. Any sanctions imposed will be adjusted according to the context of the offence, including past disciplinary history. In all cases, education as to the importance of appropriate use of electronic devices will be provided.

Date of this policy:	January 2018
Policy drawn up by:	CWS / JMG / TJGG / JCB
Date of next policy review:	March 2019
Date for publication of revised policy:	April 2019

References

Internal

- Anti-Bullying Policy
- Code of Behaviour Policy
- Eastbourne College Rules
- Cyber-Bullying Policy
- Discipline and Exclusions Policy
- Drugs and Substances Policy
- ICT Acceptable Use Policy for Pupils
- Mobile Phone and Mobile Devices Policy
- Prevent Policy
- Restraints Policy
- Safeguarding and Child Protection Policy
- Searching and Confiscation Policy
- Sexting Policy
- White Book

External

- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/488034/Behaviour_and_Discipline_in_Schools_-_A_guide_for_headteachers_and_School_Staff.pdf
- ISI Handbook for the Inspection of Schools - Commentary on the Regulatory Requirements January 2017
- Communications Act 2003: <http://www.legislation.gov.uk/ukpga/2003/21/contents>
- Computer Misuse Act 1990: <http://www.legislation.gov.uk/ukpga/1990/18/contents>
- Human Rights Act 1998: <http://www.legislation.gov.uk/ukpga/1998/42/contents>
- Malicious Communications Act 1988: <http://www.legislation.gov.uk/ukpga/1988/27/section/1>
- Telecommunications Act 1984: <http://www.legislation.gov.uk/ukpga/1984/12/contents>
- Copyright, Designs and Patents Act 1988: <http://www.legislation.gov.uk/ukpga/1988/48/contents>
- The Data Protection Act 1998: <https://www.gov.uk/data-protection/the-data-protection-act>

- Obscene Publications Act 1959 and 1964: <http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents> and <http://www.legislation.gov.uk/ukpga/1964/74/contents>
- Protection of Children Act 1978: <http://www.legislation.gov.uk/ukpga/1978/37>
- Protection from Harassment Act 1997: <http://www.legislation.gov.uk/ukpga/1997/40/contents>
- Public Order Act 1986: <http://www.legislation.gov.uk/ukpga/1986/64>
- Racial and religious hatred Act 2006: <http://www.legislation.gov.uk/ukpga/2006/1/contents>
- Sexual Offences Act 2003: <http://www.legislation.gov.uk/ukpga/2003/42/contents>
- The Sex Discrimination Act 1975: <http://www.legislation.gov.uk/ukpga/1975/65>
- The Race Relations Act 1976: <http://www.legislation.gov.uk/ukpga/1976/74>
- The Disability Discrimination Act 1995: <http://www.legislation.gov.uk/ukpga/1995/50/contents>

I have read and understand the Eastbourne College ICT AUP and agree to follow its requirements.

Full name:

House:

Signature:

Date: