Date November 2021
Review Date November 2024
Responsibility Director of IT

Staff ICT Acceptable Use Policy

Contents

Introduction

This entire policy is intended to provide guidance on the use of IT at Epsom College by members of staff, and is subject to change. It does not form part of a member of staff's contract of employment.

Information and Communication Technology (ICT) facilities at Epsom College are provided to assist staff in their role of educating and supporting pupils. The College values staff use of ICT in this role as they communicate with pupils, staff, parents, Governors and outside contacts. Furthermore, the College seeks to encourage use of ICT in providing learning opportunities inside and outside of the classroom. Epsom College trusts staff to use ICT facilities in a respectful, sensible and lawful way.

Computers have increasingly become an integral part of our lives, both working and personal. Use of the internet, sending and receiving e-mails are very simple operations and their ease of use can be their biggest drawback. Please make sure that you are familiar with and adhere to the following policy.

This Policy applies to the use of:

- All internet and electronic mail facilities, shared computers, workstations, mobile devices, and any networks, including WiFi, connecting them provided by the College;
- All cloud services to which the College subscribes e.g. SharePoint or OneDrive
- All hardware owned, leased, rented or otherwise provided by a member of staff and connected to or otherwise accessing Epsom College networks or other facilities.

Personal devices (including hardware owned, leased, rented or otherwise provided by staff) may be directly connected to College Wi-Fi network using staff's network credentials without explicit approval of the Director of Transformation and IT or the Bursar. However, connecting any device, whether personal or owned by the College, to College's wired network i.e. into a data socket can be done only by arrangement with, and with the explicit approval of the Director of Transformation and IT or the Bursar.

The system must be used only in connection with your duties for which the College employs you.

Aims of this Policy

The aim of this policy is to clarify the procedures that all staff need to follow in order to comply with both the College policy and legal obligations. If a breach of the policy occurs, then use of the facilities may be curtailed or withdrawn and disciplinary action may follow.

Staff use of ICT facilities is governed by the terms of this policy and applies to all staff working for Epsom College. Although the policy details the use of email and internet facilities, it also applies to telephone and mobile communications, photocopiers, scanners, digital cameras, camcorders, or any another audio or visual recording, viewing or listening device.

This policy is linked to the College's Policy on Pupils' Use of ICT, Mobile Phones and Other Electronic Equipment, as well as other relevant College policies such as the Child Protection & Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Health and Safety Policy, Privacy Notice for Staff the Social Media Policy.

All members of staff have a duty to ensure that pupils using ICT, in any context, are reminded about appropriate behaviour on a regular basis. Appropriate behaviour for pupils is detailed in the Policy on Pupils' Use of ICT, Mobile Phones and Other Electronic Equipment.

Please see Appendix 1 as to how to deal with a breach of this policy by a member of staff and Appendix 2 for the procedure to follow for breach of the Policy on Pupils' Use of ICT, Mobile Phones and Other Electronic Equipment.

Staff Use of ICT

In using the College's ICT systems a member of staff is expected to:

- Observe this policy at all times and note the disciplinary consequences of non-compliance which in the case of a gross breach or repeated breach of the Policy, may lead to dismissal;
- Ensure that they use the College standard e-mail sign off and disclaimer for all external e-mail;
- Produce and write e-mail with the care normally given to any form of written communication;
- Appreciate that electronic mail is relatively insecure and consider security needs and confidentiality before transmission.

Use of Electronic Mail

Emails should be treated in the same way as any other form of written communication. Staff should not include anything in an email that would not be appropriate to be published generally.

College email accounts are to be used for College business. Limited personal use is considered acceptable.

All staff should

- Not send or receive messages that are offensive, obscene, defamatory, abusive or otherwise unlawful. Emails, like any other form of written communication, can be used as evidence in a court of law;
- Not represent personal opinions as those of the College;
- Not send unsolicited commercial or advertising material;
- Use the standardised College email signature;
- Not amend any messages received and, except where specifically authorised by the other person, not access any other person's email nor send any email purporting to come from another person;

The College does not take any responsibility for any offence caused by staff members as a result of downloading, viewing or forwarding inappropriate emails. Please be aware that trivial messages and jokes should not be sent or forwarded by email to avoid over-burdening the IT system.

Our internal email traffic is encrypted preventing unauthorised access, however, email is not a confidential means of communication and emails can be:

- Intercepted by third parties (legally or otherwise);
- Wrongly addressed;
- Forwarded accidentally;
- Forwarded by initial recipients to third parties against your wishes;
- Viewed accidentally on recipients' computer screens.

This should be considered when sending confidential information via email.

Emails may be disclosed in response to subject access request, and all members of staff should remember that there is no exception from disclosure for embarrassing or damaging content. Staff are expected to consider this carefully before committing something to email or any electronic forum if they would not say it to the individual

concerned or write it in a letter. Staff should be aware that there is no expectation that the content of an email will remain confidential if it contains personal data relating to another individual, particularly if legal proceedings proceeding are instigated as all emails and communications are potentially disclosable.

Use of the Internet and Intranet

Access to certain websites is filtered for security and legal purposes. If staff need to access a blocked site, they should contact the IT Department, who will confirm whether the site can be unblocked.

Staff must not:

- Intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software;
- Seek to gain access to restricted areas of Epsom College's network;
- Access, or try to access, data which they know, or ought to know, is confidential;
- Carry out any hacking activities or introduce packet-sniffing or password-detecting software;
- Seek to gain access to unfiltered material (e.g. by the use of proxies or VPN services).

Staff should not enter into any contract or subscription on the internet on behalf of the College unless express approval has been granted in advance by the Director of Transformation and IT or Bursar.

Personal Blogs and Websites

This applies to content that a member of staff may publish on the internet (e.g. contributions to blogs, message boards, social networking or content-sharing sites) unless it is an Epsom College approved site. It does not include the use of LinkedIn for professional reasons, but would include any comments or remarks made on LinkedIn.

- If a member of staff posts any content which identifies (or could identify) them as a member of Epsom College staff and/or they discuss anything related to Epsom College (or its pupils, staff, Governors or parents), the College expects the member of staff to conduct themselves appropriately and in a manner which is consistent with College's policies and procedures;
- If a posting clearly identifies that the member of staff works for Epsom College and they express any idea or opinion, then they should add a disclaimer (e.g. "these are my own personal views and not those of Epsom College");
- If they already have (or intend to have) a personal blog or website which indicates in any way that they work for Epsom College, then they should ask permission from/report this to the Second Master.

The following matters will be treated as possible matters for disciplinary action (this list is not exhaustive):

- Revealing confidential information about Epsom College or information relating to pupils, staff, Governors or parents;
- Causing disrespect to the College, or its pupils, staff, Governors or parents (e.g. through comments that criticise or embarrass said parties).

If someone from the media contacts a member of staff about any publication that relates to Epsom College or the member of staff has any concerns or are unclear about any of the above points, then they should talk to the Second Master.

Misuse of Epsom College Facilities and Systems

Members of staff must not misuse the College's facilities and systems.

Misuse of facilities covers the viewing, accessing, transmitting, posting, downloading or uploading of any of the following (this list is not exhaustive):

- Offensive, obscene, derogatory or unlawful material or material which is liable to cause embarrassment or bring the reputation of the College (or any of its pupils, staff, Governors or parents) into disrepute;
- Material which is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/or offensive;
- The viewing, posting, uploading or downloading terrorist or extremist material;
- Any defamatory material about any person or organisation, or material which includes statements which are untrue or of a deceptive nature;
- Confidential information about Epsom College and any of its pupils, staff, Governors or parents;
- Accessing or communicating with pupils via social media;
- Any material which, by intent or otherwise, inconveniences, causes distress or harasses the recipient;
- Any material which violates the privacy of others or misrepresents others;
- Any other statement which is likely to create any liability;
- Material in breach of copyright and/or other intellectual property rights;
- Online gambling, unsolicited commercial or advertising material, chain letters or other junk mail.

Viewing unsuitable material online (e.g. obscene or unlawful material) is strictly prohibited and is classed as gross misconduct under the College's Disciplinary Procedures, and could therefore result in the dismissal of the employee concerned.

Staff must not:

- Use networked computing equipment for playing computer games;
- Gain deliberate unauthorised access to facilities or services accessible via local or national networks;
- Gain unauthorised access to or violate the privacy of other people's files, corrupt or destroy other people's data or disrupt the work of other people;
- Disclose passwords to third parties without the consent of the College;
- Download any file or programme that is not specifically related to their job.

Epsom College's facilities must not be used in connection with the operation of any business or used in any way which may cause damage or overloading of the facilities, or which may affect performance.

Working Remotely

This applies to the use of College systems and to a member of staff's use of personal or another person's equipment (e.g. a colleague's equipment) when they are working on College business away from College premises.

When a member of staff is working remotely they must:

- Password-protect any College-related work so that no other person can access it (and keep their passwords secret);
- Make sure no personal or sensitive information regarding pupils or staff is stored locally on the remote computer or any removable devices e.g. USB key. If it is absolutely necessary to store personal or sensitive data on a removable device this must be encrypted without exception.
- Position themselves so that their work cannot be seen by any other person;
- Take reasonable precautions to safeguard the security of equipment (e.g. their laptop);
- Inform the IT Department as soon as possible if a College laptop (or any computer equipment which holds College related work) has been lost or stolen;
- Ensure that any work carried out remotely is saved on to the College's system, or is transferred to the College system as soon as reasonably practicable.

Personal Use

Although Epsom College's ICT facilities are provided for the purposes of education, a certain amount of limited, and responsible, personal use is permitted, but this is a privilege and not a right and may therefore be removed if a member of staff is found abusing this privilege.

The College may need to monitor communications for the reasons given below.

Staff must ensure that personal use:

- Does not interfere with the performance of their duties;
- Is minimal, and limited to taking place substantially outside of normal working hours (i.e. during any breaks, or before or after normal hours of work);
- It is clear from the email title that this is a personal email, and not one sent on behalf of Epsom College. Staff are therefore encouraged to mark the email as Personal in the subject box.
- Does not cause unwarranted expense or liability to be incurred by Epsom College.

Monitoring of Communications by Epsom College

The College is responsible for all communications, but subject to that will, so far as possible and appropriate, respect a member of staff's privacy while they are working.

The College reserves the right to monitor all communication and activity, both inside and outside of working hours, on all College issued devices or devises used for College purposes such as mobile telephones, tablets and laptops.

The College reserves the right to monitor staff communications in order to:

- Establish the existence of facts;
- Ascertain compliance with regulatory or self-regulatory procedures;
- Monitor standards which are achieved by persons using the system in the course of their duties and for staff training purposes;
- To prevent or detect crime;
- To investigate or detect unauthorised use of the College's telecommunication system;
- Ensuring the effective operation of the system such as protecting against viruses, backing up and making routine interceptions such as forwarding e-mails to correct destinations;
- To check compliance with all of the College's policies and to help fulfil its legal obligations;
- To gain access to routine business communications for instance checking voice mail and e-mail when staff are on holiday or on sick leave

Epsom College will monitor telephone, email and internet traffic (e.g. websites visited, duration of visits, and files downloaded), covering both personal and professional communications, for the purposes specified above. By using Epsom College's facilities, a member of staff consents to the College processing any personal data which may be revealed by such monitoring. To maintain a member of staff's own personal privacy, staff need to be aware that such monitoring might reveal personal data about them.

Any emails which are not stored in a "Personal" folder in a school mailbox and which are not marked PERSONAL in the subject heading will be treated, for the purpose of availability for monitoring, as professional communications. In certain very limited circumstances the College may, subject to compliance with any legal requirements, access email marked PERSONAL. For example, when there is reasonable suspicion that emails may reveal evidence of inappropriate activity.

Sometimes it is necessary for the College to access a member staff's communications during their absence, e.g. when they are away ill or on holiday. Unless mailbox settings are such that the individuals who need to do this already have permission from the member of staff concerned to view their inbox, access will be granted only with the permission of one a member of the Senior Leadership Team who are authorised to grant such access.

All incoming emails are scanned using virus-checking software. The software will also block unsolicited marketing emails (spam) and emails which have potentially inappropriate attachments. If there is a suspected virus in an email which has been sent to a member of staff, the sender will automatically be notified and the member of staff will receive notice that the email is not going to be delivered to them.

Data Protection

Data protection concerns the privacy of individuals, and is governed by the Data Protection Act 2018. The relevant points of the Data Protection Act are:

- Staff have the right to see all the information held about them;
- It is a criminal offence to obtain or disclose personal data without the consent of the College.

A member of staff may be committing this offence if, without authority of Epsom College:

- They exceed their authority in collecting personal data;
- They access personal data held by Epsom College, control it or pass data on to someone else.

For further information, please refer to the College's Data Protection Policy and Privacy Notices for Staff, Pupils and Parents which can be found on the Intranet homepage, the College website or obtained from the Bursar's office.

Treatment of IT Equipment and Security

Staff are required to treat IT equipment belonging to the College with respect and reasonable care, and to report any faults or breakages immediately.

Computer screens should be locked when a member of staff leaves their computer or device in order to prevent unauthorised or accidental access to sensitive information and staff are strongly advised not to use obvious passwords. If a member of staff suspects that a third party knows their password they should report it to the Director of IT and change their password immediately;

Staff are required to change their passwords in accordance with College's password policy. In exceptional circumstances e.g. real or perceived security threat, the College reserves the right to insist on password change with immediate effect.

Compliance with this Policy

Failure to comply with this policy may result in disciplinary action being taken against you under Epsom College's disciplinary procedures.

If a member of staff has any queries about the policy, would like further information, or are in doubt about a course of action, take advice from your Head of Department, or contact the Second Master or Director of Transformation and IT.

If you need any technical guidance, contact the IT Department.

Please note that the procedures and policies outlined in this policy, and in any related policy, may be reviewed or changed at any time. Staff will be alerted to important changes, whilst updates will be made to the appropriate files.

Appendix 1

Reporting Processes for Breach of Staff ICT Acceptable Use Policy

In all circumstances, report the incident to the Second Master or a member of the Senior Leadership Team.

The Second Master or the member of the Senior Leadership Team must:

- Log and reference the incident;
- Review the incident and decide on the appropriate course of action;
- Investigate whether any changes need to be made to any policies or technical tools (in discussion with the Director of Transformation and IT, where appropriate).

Where necessary, report the misuse to the Internet Watch Foundation website at https://www.iwf.org.uk (who will advise what to do next).

Note

- If the material is on the Internet, do not show anyone the content or make the web address public;
- If the material is an image in the body of an email, close the email; under no circumstances forward the email, copy the image or show it to another person, as each of these actions constitutes an illegal offence;
- Any person suspecting another of deliberate misuse or abuse must report in confidence to the Second Master or a member of the Senior Leadership Team (who must then follow the process above);
- Any breach of unauthorised use will be reported by Director of Transformation and IT to the Second Master or a member of the Senior Leadership Team (who must then follow the process above).

Appendix 2

Reporting a Breach of Pupils' Use of ICT, Mobile Phones and Other Electronic Equipment

In all circumstances, report the incident to the Second Master and the pupil's Housemaster or Housemistress.

The Second Master must:

- Log and reference the incident;
- Review the incident and decide on appropriate sanctions or course of action;
- Inform the Director of Transformation and IT (who will help investigate whether any policy or technical changes need to be made).

Where necessary, report the misuse to the Internet Watch Foundation website at https://www.iwf.org.uk (who will advise what to do next).

Any breach of unauthorised pupil use will be reported by the IT Department to the Second Master (who must then follow the process above).

Note

- If the material is on the Internet, do not show anyone the content or make the web address public;
- If the material is an image in the body of an email, close the email; under no circumstances forward the email, copy the image or show it to another person, as each of these actions constitutes an illegal offence.