Kingswood College Policy

ELECTRONIC COMMUNICATION, INTERNET, SOCIAL MEDIA AND WEARABLE TECHNOLOGY USER POLICY

RESPONSIBILITY

Author: Mrs Soné Griesel
Date implemented: 04 February 2021
Approved by:

REVIEW

Last Review date: 04 February 2021
Next review date:

INTRODUCTION

This is a general policy that highlights some aspects of employees'/pupils' use of computers, communication systems, digital devices, internet, social media, etc.
The School has detailed policies on ICT security, restricted use of computer/digital equipment, firewalls, passwords, etc., which are extremely important and must be strictly adhered to at all times. Employees/pupils must familiarise themselves with the relevant policies, which can be obtained from the IT department. If there is a conflict between this policy and any of the specific ITC policies, the latter shall prevail.

GENERAL PRINCIPLES

1. Computers and electronic equipment (including telephones, smart devices, etc.) may be made available to employees/pupils for the express purpose of the School's educational and business use. Employees/pupils are therefore required to utilise this equipment in a responsible and productive manner, and for the purpose intended. Personal use of School equipment (including telephones) is subject to authorisation and employees/pupils may be required to reimburse the School for such use. Excessive use or abuse of the School's equipment or systems will be subject to disciplinary action.

2. Use of School equipment is also subject to the operation of equipment in a safe and proper manner, and any other conditions of use as set out in this policy. Many of the systems and software programmes used by employees/pupils at the School may be "shared services", and it is crucial that all system users personally take adequate measures to maintain the integrity and security of these systems.

3. Any abuse or commercial use of such equipment, or private use thereof to the extent that it impacts negatively upon the School and/or could be potentially harmful, shall be treated as misconduct. This includes committing, facilitating or enabling any form or intrusion, hacking, unauthorised access or the like.

4. The School has the right to monitor, access and review the utilisation of all its computer, communication or similar equipment without notifying employees/pupils. In terms of employees'/pupils' consent to the monitoring and interception by the School of their usage and communications this includes all and any e-mail, voice-mail, internet, text messages and other electronic records. The information so obtained may be used for any legitimate purpose by the School, and such use will not constitute a breach of employee/pupil privacy.

5. Employees/pupils are responsible for their behaviour on school computers and/or any electronic- and communication devices. They are expected to behave in accordance with the Code of Conduct of the School and their contract of employment/internet & computer acceptable use agreement and to observe the rules that apply to computer, electronic media and internet usage.

6. Employees/Pupils who use electronic equipment, access the internet, play games, listen to or download music, participate in social media, take photographs, make recordings or send electronic messages via digital devices or similar, even in their private capacity or using their own equipment, may not do so in any way that prejudice or impact negatively on the School or its interests, or compromise confidentiality or private information. Such conduct will entitle the School to institute a disciplinary investigation against the employee/pupil.

SPECIFIC RULES

7. **KINGSWOOD COLLEGE will, *inter alia*, not permit the following:**

7.1. The display, transmission, accessing, viewing, storing, downloading or creation of inappropriate or private material, including:

- material that is harassing, embarrassing, lewd, suggestive, unlawful, inappropriate or pornographic (including writings, pictures, films, video clips of a sexually explicit or arousing nature);
- offensive, obscene, discriminatory, fraudulent or criminal material or material which is liable to cause embarrassment to the School or its stakeholders, or material which is derogatory or may cause embarrassment to others;
- false and/or defamatory statements about any person or organisation, or any other statement which is likely to create any liability (whether criminal or civil), for the employee or the School;

7.2. Engaging in online gambling, games, chain letters, unauthorised use of chat programs or e-mail other than the School's approved e-mail etc.

7.3. The unauthorised access, duplication or dissemination of copyrighted or patented software, documents, data or recordings; any form of plagiarism. The School does not accept responsibility for any action or liability incurred by an employee/pupil who acts in a manner that breaches this policy.

7.4. Use of another person's password or any unauthorised attempt to gain access to or modify another person's work.

7.5. Damaging or changing the configuration of computers, computer systems or the computer network, including both hardware and software; unauthorised installation of software on the School's computers.

7.6. Malicious use of the network to infiltrate a computer system; the transmission or creation of any virus, worm, Trojan horse or any other destructive code.

8. **Emails**

8.1. Electronic messages should be concise and directed only to relevant individuals. Care must be taken when forwarding or replying to e-mails or text messages, that message strings are not inadvertently included when (some of) the recipients have no reason to see these and such previous communications are confidential, private or irrelevant.

8.2. Before sending, forwarding or replying to any electronic message, employees/pupils must ensure that all of the information contained in that message (including the e-mail addresses or telephone numbers of other participants in the message string) -

- is intended for each individual recipient;
- is not subject to privacy or confidentiality restrictions; or
- is not in contravention of laws or regulations pertaining to the protection of personal information.

8.3. Employees should endeavor to access their e-mails regularly every working day, stay in touch by remote access when travelling and use an out of office response when away from work for more than a day and are unable to respond to e-mail.

8.4. Employees/pupils should not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory or otherwise inappropriate messages and if such messages are received, not forward them but report this to the IT administrator. Employees/pupils should assume that e-mail, text / voice messages may be accessed by others and not include in them anything which would offend or embarrass any person, or themselves, if it found its way into the public domain.

8.5. E-mail or other electronic messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail or message is obliterated and all messages should be treated as potentially retrievable, either from the main server or using specialist software.

8.6. In general, employees/pupils, as users of the system, may not:

- Send or forward private electronic messages at work which they would not want a third party to read; or send private messages which reflects the School's name or details anywhere;
- Send or forward electronic messages circulated within the School to an external user of the system without the express prior written permission of the author.
- Send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the School;
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;
- Agree to terms, enter into contractual commitments or make representations by e-mail or electronic message unless appropriate authority has been obtained, as a name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter;
- Access by use of a password or send messages from another employee's computer/device or under an assumed name unless specifically authorised;
- Send confidential messages via e-mail, the internet, digital messaging or by other means of external communication which are known not to be secure.

8.7. Employees/pupils who receive an electronic communication which has been wrongly delivered should return it to the sender of the message. If the communication contains confidential information or inappropriate material, it should not be disclosed or used in any way.

Violations of the above rules will result in disciplinary action.

9. Please note**:**

9.1. Users are responsible for any misconduct while a computer/electronic device is logged in under their name.

9.2. The network administrator has the right to monitor all accounts and the use of the Internet, if authorised to do so by the Head.

9.3. The network administrator, after giving prior notice, has the right to delete inactive files.

9.4. Employees/pupils are required to follow any instruction with regard to their use of the Internet given by the network administrator or a member of management.

9.5. Whilst all reasonable steps are taken to ensure compliance with these rules, the School will not be held responsible for any loss or damage of any nature whatsoever arising from a breach of these rules by any person.

SOCIAL MEDIA

10. The School recognises the evolution of social media as a mechanism of communication and it is important to that social media be used responsibly and appropriately in relation to the School's business and the larger school community. This also applies to chat applications such as WhatsApp groups.

11. It is important for employees/pupils to understand both the advantages and the potential risks of social media, so that they may enhance their use thereof and avoid or mitigate the risks inherent in social media. Even private messages or posts could become public via screen grabs and publication by others.

12. Employees/pupils using any social media platforms for purposes related to their employment at the School or which may in any manner link such use with the School, shall:

    - if they have the authority to make statements on behalf of the School, clearly indicate such authority (statements to the media must first be approved by the employer);
    - if they do not have authority to make statements on behalf of the School, clearly indicate that the statement is their own opinion and does not represent the School or any other person at the School;
    - only use the official and approved logo / branding;
    - adhere to relevant policies, procedures and standards adopted by the School governing the publication of School information, its information security and communications by employees;
    - strictly observe all confidentiality obligations and not communicate any confidential information using social media or any other communication platforms;
    - ensure that the contents of postings are accurate, ethical and legal;
    - not post:
        - information which may be detrimental to the School, any of its employees or stakeholders;
        - information or comments pertaining to colleagues, fellow pupils;
        - any person's / learner's private information (including photographs or images where the person is visible) of whatever nature, without the authority of the person / parent / guardian;
        - any inappropriate, suggestive, obscene or pornographic images;
        - any communication or image which may be defamatory or violate the rights of any party;
        - any communication which is offensive, threatening, abusive, harmful, hateful, malicious, discriminatory, demeaning, derogatory or which amounts to unlawful harassment or unfair discrimination;
        - illicit photos, profanity or other derogatory content;
        - a communication which violates the intellectual property rights of third parties.
    - regularly review the content of social media postings and remove any information that could reflect negatively on the School or its clients (for example inappropriate comments made in response to postings);
    - always log out of social media applications when use of the application has been completed;
    - not use social media platforms to communicate unsolicited communications of whatever manner; and
    - not impersonate third parties or act in any manner that may mislead, confuse or deceive others;

- not engage in online communication activities which could bring the School into disrepute.

13. Employees using social media platforms for non-business purposes may be accountable to the School if they use the School's equipment to access such sites; and/or if they access such sites during work hours (even if using their own equipment) in any manner that interferes with the proper performance of their duties.

14. Employees'/pupils' postings on personal social media platforms may also not in any way impact negatively on the School or anyone related to / associated with the School.

    Employees/pupils should be aware that any conduct, even in their private capacity, which impacts on the interests of the School, must be in accordance with the School's rules and policies. In circumstances where an employee/pupil, for example, defames or discloses confidential information on a social network and this causes damage to the School's reputation and/or results in the loss of business, this could potentially destroy the trust relationship between the School and the employee and make continued employment impossible.

15. Employees/pupils should take care to utilise privacy settings and to lock access to their profiles for users that they do not know.

16. Employees/pupils should not create School-related chat-groups (e.g. with co-workers, or parents, or learners) unless this has first been cleared with the College Head or Management Team*;* and should not add any person to such a group unless they had an opportunity to consent or decline being added.