Kingswood House School

USE OF TELEPHONE, E-MAIL SYSTEMS AND INTERNET

This policy relates to the whole school including the Early Years Foundation Stage.

Created by **Sally Witts**
Date **July 2022**
Review date **July 2023**

Our IT and communications systems are intended to promote effective communication and working practices within the School. This policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor your use, and the action we will take in respect of breaches of these standards.

This Policy applies to the use of:

- all internet and electronic mail facilities, multi-user computers, workstations, micro-computers, and any networks connecting them provided by the School; and

- all hardware owned, leased, rented or otherwise provided by a member of staff and connected to or otherwise accessing School networks or other facilities

Hardware owned, leased, rented or otherwise provided by staff may be directly connected only by arrangement with, and with the explicit approval of the Bursar.

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

Limited use of E-mail and Internet facilities for personal purposes is permitted. The School acknowledges that personal use may occur from time to time. Any such use must be in accordance with this Policy and must not disrupt staff duties. Abuse or excessive use of the e-mail and/or Internet will be dealt with through the disciplinary procedure.

You must not interfere with the work of others or the system itself. The facilities must be used in a responsible manner - in particular, you must not:

- create, transmit or cause to be transmitted material which is designed or likely to cause annoyance, inconvenience, needless anxiety or offence, and you

must not create, transmit or cause to be transmitted offensive, obscene or indecent material;

- create, transmit or cause to be transmitted defamatory material;
- create, transmit or cause to be transmitted material such that the copyright of another person is infringed;
- download any files unless virus scanned;
- use networked computing equipment for playing computer games;
- gain deliberate unauthorised access to facilities or services accessible via local or national networks;
- transmit by e-mail any confidential information of the School otherwise than in the normal course of your duties;
- send any message internally or externally which is abusive, humiliating, hostile or intimidating;
- join any mailing groups or lists without the consent of the School.
- 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 School.

You must:

- 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 you use the School standard e-mail sign off and disclaimer for all external e-mail;
- produce and write e-mails 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.

Monitoring

The School's systems enable us to monitor telephone, email, voicemail, internet and other communications. For business reasons, and in order to carry out our legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise.

Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

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

- estalish 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;
- prevent or detect crime;
- investigate or detect unauthorised use of the School's telecommunication system;
- ensure 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; and
- gain access to routine business communications for instance checking voice mail and e-mail when staff are on holiday or on sick leave.

A CCTV system monitors the exterior of the School 24 hours a day. This data is recorded.

We reserve the right to retrieve the contents of email messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

- to monitor whether the use of the email system or the internet is legitimate and in accordance with this policy;

- to find lost messages or to retrieve messages lost due to computer failure;
- to assist in the investigation of alleged wrongdoing; or
- to comply with any legal obligation.

Equipment Security and Passwords

You are responsible for the security of the equipment allocated to or used by you, and must not allow it to be used by anyone other than in accordance with this policy.

You are responsible for the security of any computer terminal used by you. You should lock your terminal or log off when leaving it unattended or on leaving the School, to prevent unauthorised users accessing the system in your absence. Anyone who is not authorised to access our network should only be allowed to use computer terminals under supervision.

Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the Head of IT.

You should use passwords on all IT equipment, particularly items that you take out of School. You must keep your passwords confidential and change them regularly. You must not use another person's username and password or make available or allow anyone else to log on using your username and password unless authorised by the Head of IT. On the termination of employment (for any reason) you must provide details of your passwords to the Head of IT and return any equipment, key fobs or cards.

If you have been issued with a laptop, tablet computer, smartphone or other mobile device, you must ensure that it is kept secure at all times, especially when travelling.

Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

Systems and data security

You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

You must not download or install software from external sources without authorisation from the Head of IT. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming

files and data should always be virus-checked by the IT Department before they are downloaded. If in doubt, staff should seek advice from the Head of IT.

You must not attach any device or equipment to our systems without authorisation from the Head of IT. This includes any USB flash drive, MP3 player, tablet, smartphone or other similar device, whether connected via the USB port, infra-red connection or in any other way.

We monitor all emails passing through our system for viruses. You should exercise particular caution when opening unsolicited emails from unknown sources or an email which appears suspicious (for example, if it contains a file whose name ends in .exe). Inform the Head of IT immediately if you suspect your computer may have a virus. We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties.

You must be particularly vigilant if you use our IT equipment outside the workplace and take such precautions as we may require from time to time against importing viruses or compromising system security. The system contains information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.