POLICY TITLE: ELECTRONIC ACCEPTABLE USE (STAFF) POLICY

DEVELOPED/REVIEWED BY

Director of Digital Engagement
Senior Leadership Team

REVIEW SUMMARY

The electronic communication and information resources of The King David School are part of the School's educational resources. These resources are made available to enhance the educational experiences of students and to provide staff members, and independent contractors where engaged, with the tools necessary to implement and enhance the School's educational program.

DOCUMENT DEVELOPMENT PROCESS

This document was reviewed in April 2023 by the Director of Digital Engagement with no adjustments made.

RATIONALE

This Policy specifies the conditions applying to the use of the technology resources. This includes the computer network, internet access, computers and other communication devices, including but not limited to:

- Computers, laptops, tablet devices;
- External storage devices
- cameras (such as video, digital, webcams);
- all types of mobile phones;
- gaming consoles;
- video and audio players/receivers (such as portable CD and DVD players); and
- any other similar technologies, as they come into use.

The technology resources include but are not limited to all Internet, Intranet and /or communications and all related applications, such as the following:

- email;
- staff, student and parent portal;
- Google Workspace Products
- electronic discussions/newsgroups/bulletins;
- downloading or accessing files from the Internet or other electronic sources;
- publishing and browsing on the Internet (including Intranet);
- files transfer;
- file storage;
- file sharing;
- instant messaging;

- copying, saving and distributing files;
- viewing material electronically;
- printing material;
- subscriptions to list servers, mailing lists or other like services;
- blogs;
- social media
- video conferencing; and
- streaming media.

The technology resources are available for the use of employees under the conditions specified in this Policy. This Policy is to be read in conjunction with other statements and policies made by the School and may be amended from time to time.

Authorised users of the School's technology resources are required to comply with this Policy. Failure to observe this Policy will result in disciplinary action that could include termination of employment.

DEFINITIONS

digital technology	Includes ICT, social media, online games, file and information sharing applications, messengers, multimedia, productivity applications, cloud computing and interoperable systems that store, retrieve, manipulate, transmit or receive digital resources.
digital resources	Files or signals in a digital format that can be accessed, stored, manipulated or transmitted electronically. These may include but not limited to: data, sound, maps, animation/video, photos, sound, images, common application files like MS Excel, MS Word and Adobe PDF.
electronic communication platform	A system for sending and receiving messages electronically over a computer network.
information communication technology (ICT)	Any technology or device that will or can store, retrieve, manipulate, transmit or receive information or digital media electronically, this includes, but is not limited to, telephones, mobile phones, computers (servers, desktops, laptops, tablets), printers, scanners, wireless or computer networks, broadcasting equipment, software, middleware, storage, audio-visual systems, electronic communication platforms , internet, intranet and extranets.
intranet	A privately maintained computer network that can be accessed only by authorised persons, such as members of The King David School community.
password	A code, which, when associated with a user account, provides access to digital technology, through an authentication mechanism or a login page.
users	Are College employees, contracted staff and any other persons authorised by the College accessing College digital technology.

PRINCIPLES/GUIDING PRINCIPLES

- The School's digital technology tools are to be used to assist in a manner that is consistent with the expectations of The king David School Values
- Subject to the School's rights under this Policy, the School respects the privacy and confidentiality of users' data and restricted access is provided by means of user passwords
- Pre-service teachers and other persons may be given temporary, designated access to School digital technology at the discretion of the Principal or delegated nominee
- Users of School digital technology must abide by relevant laws, legislation and School policies and guidelines. Users are required to make use of these facilities in a manner that it ethical, legal and does not interfere with use by others
- All messages and digital resources composed, sent or received on the School's electronic communications platform are and remain the property of the School. They are not provate property of any user

- The School reserves the right to monitor the use of the School's digital technology to the extent allowed by relevant laws and to ensure compliance with School policies. This includes remote access
- Compliance with this policy and related guidelines, as may be updated from time to time, is a condition of employment with the School. Any breaches of this policy may result in disciplinary action which may include termination
- Users must protect passwords at all times against disclosure or unauthorised use, including generated, distributed, used and stored

Users must comply with the requirements of any School policies or guidelines relating to use of digital technology and/or password creation, management and protection, as may be updated from time to time.

PROCEDURES

Authorised Use

Authorised users of the technology resources for legitimate work-related purposes are those people issued with a valid username and a password.

Employees are responsible for maintaining the security of their accounts and their passwords. Passwords are required to be changed regularly. All employees are required to take appropriate precautions to prevent unauthorised access to their account by logging off whenever the accessed terminal or device is unattended.

Usage

The technology resources are an important component of the School's internal and external communication systems. This system is available to employees to facilitate efficient communication for work-related purposes.

Authorised users may use the technology resources for reasonable personal purposes. Reasonable personal use means use for non-work work related purposes including Internet usage and private emails. Such use must not contravene this Policy or have any foreseen or unforeseen negative ramifications for the School. Further, such use must not adversely affect, or have the potential to adversely affect, personal productivity and professional standards. Use may include personal transactions with online financial institutions.

Personal use of the School's technology resources will be acknowledgement that authorised users will be personally accountable for any costs or other negative ramifications that may result from using the system.

As the School owns its technology resources, the contents of the system, including email messages and the historical log of electronic communications, are the property of the School. Any document, data or other material created, stored and/or transmitted with School-owned or leased information technology is considered TKDS' information. That information may be viewed by TKDS staff, even if created in an employee's "personal" computer storage area. Privately owned machines that are connected via the School's network infrastructure or contain School records become available to authorised TKDS' staff.

The School reserves the right, through authorised personnel, to monitor the usage of its technology resources, including the tracking of individual usage. Information stored on the School's technology resources may be inspected and disclosed during routine monitoring or where misconduct/misuse is suspected, in response to legal processes and/or to fulfil obligations to a third party. At any time, School devices may be remotely controlled by the IT department to fix software problems and to monitor computer use.

Storage

All employees of KDS are required to have their documents stored in the KDS Google Drive, Shared network drives or School approved curriculum or learning management systems, and not external storage media or unauthorised cloud-based storage, such as iCloud, Dropbox etc.

Good Practice and Etiquette Governing Email Use

Care should be taken to ensure that the content, form, grammar and spelling of all email messages meet the professional business standards required by the School for all forms of correspondence and comply with all statutory obligations.

All users are reminded that electronic communications may not be secure, and from time to time, communications may find their way to an audience beyond that originally intended. For example, electronic communications are capable of being forwarded without the express permission of the original author. Therefore, users must exercise caution in the transmission of messages.

Where the author of a document wishes to minimise the possibility of a document being altered by the recipient, the document should be sent in a format with protection from alterations. This format should be adopted where the School seeks to protect its intellectual property.

Differentiating between Personal Correspondence and Authorised Representation

As each authorised user is identifiable as having an account at The King David School, it is necessary to differentiate between personal views and opinions and the official views of the School.

The Principal or authorised agent may specifically delegate responsibility to authorised employees to represent the School in a professional capacity from time to time. In other circumstances, a disclaimer advising that the views and opinions expressed represent those of the writer and not the School, is required.

Form of Messages

All messages should contain:

- appropriate salutations;
- sender’s name and title (and POR, where relevant);
- name and contact details of the School;
- standard School disclaimer

Publishing

Authorised users wishing to use the School’s technology resources to publish information relating to, and on behalf of the School, must obtain prior permission from the Principal or authorised agent.

The School logo and designs are the property of the School and may only be used with the express authorisation of the Principal or authorised agent.

Communication with the School Community

Authorised users are expected to acknowledge electronic communications from the School Community. Where a direct response is not appropriate, the staff member is expected to provide a polite reply acknowledging the inquiry and indicating that a formal reply will follow.

Communication with Parents

Where parents communicate with members of staff via email, staff members must observe the following guidelines:

- The staff member is required to acknowledge receipt.
- The Principal or their authorised delegate must approve any communication concerning matters relating to School policy.
- Staff members should be wary of providing advice by Email. Advice is often best communicated in discussion, whether in person or by telephone.
- Correspondence with the family that is important for the ongoing academic and wellbeing needs of a student is required to be stored on the student profile of the staff portal.

Communication with Students
Staff members are required to maintain the highest standards of professional conduct when communicating with students electronically, as email provides students with a permanent record, in writing.

All communication with students is to be respectful and constructive. Staff members are specifically advised to refrain from any comments that are familiar or may embarrass, humiliate, intimidate or harm a student. As role models, our staff must ensure that they use language which promotes respect and is unbiased and courteous.

Electronic communication via social media presents a number of potential pitfalls: staff are specifically advised that they are not to become friends with students on Facebook, Instagram, Snapchat or any other social media apps or platforms, or add them to their list of contacts in any social media.

The following procedures must be adhered to at all times in respect of social media unless otherwise authorised by the Principal for official school purposes.

- Staff should not communicate with students using any social media (e.g. Facebook, Instagram, Twitter, Skype, etc.), or via any messaging except for Google Workspace.
- Teachers must only communicate with students via email using School email accounts. Communication between teachers and students via private email is prohibited.
- Teachers should not give students their mobile numbers and they should not SMS students. A School mobile is available for teachers to use on excursions and camps.
- Teachers should not be on social media with former students of the School for 2 years after they have graduated the School.

Communication between Staff

- Staff should only use Google Workspace products for communicating with other staff members regarding school-related business (such as Camps, Excursions, etc). Other forms of communication, such as Signal, Facebook Messenger, Instagram, What's App groups, etc, are not permitted.

Acceptable and Unacceptable Electronic Communications

Acceptable messages include:

- replying to messages, provided the reply does not contravene this Policy or any other policy of the School;
- contacting persons/organisations for legitimate and reasonable work-related purposes; and
- reasonable personal use, as outlined above.

Unacceptable messages include:

- ordering any product or service on behalf of the School unless specifically authorised;
- highly confidential information, unless encryption has been enabled; and
- any prohibited use, as outlined under 'Prohibited Use of Technology resources".

The use of any personal equipment/devices/peripherals (including any electronic storage facility) used at school, or at any school-related activity, must be appropriate to the School environment. This includes any images or material present/stored on personal equipment/devices/peripherals brought onto the School site, or at any school-related activity. This also includes the use of mobile phones.

Authorised users must not attempt to download, install or connect any software or hardware onto School technology resources, or utilise such software/hardware, unless authorised by the ICT Manager.

Prohibited Use of the Technology resources

Electronic messages are neither private nor secret and can be easily misconstrued by recipients or mistakenly sent to the wrong recipient. In Australia, State and Federal legislation prohibits the transmission of email messages that contain objectionable material. For example, emails that may appear humorous and innocent to some people can be unlawful and infringe racial and sexual discrimination and harassment policies.

Prohibited uses of the School's technology resources include any conduct that:

a. violates or infringes the rights of any other person, including the right to privacy. Staff are prohibited from spreading gossip and/or personal or confidential information about another employee, except on limited occasions with their prior approval. Examples of such occasions may include the birth of a child or the death of a family member. Protecting employees' privacy is an obligation that employees and managers must honour.

b. contains real or potentially defamatory, false, inaccurate, abusive, obscene, violent, pornographic, profane, sexually-explicit, sexually-oriented, threatening, racially-offensive or otherwise biased, discriminatory or illegal or any other inappropriate material;

c. has instructions on the manufacture and/or use of illegal and/or dangerous products, substances or materials or any other illegal or subversive activity;

d. involves gambling, or actions that could be construed as gambling;

e. violates any other School policy, including prohibitions against harassment of any kind;

f. sends confidential messages and information to personnel to whom transmission was never authorised by the School, including persons within the School Community and persons/organisations outside that Community;

g. accesses copyright information in a way that violates copyright. The copyright material of third parties (e.g., software, articles, graphic files, music files, database files, video files, text and downloaded information, etc.) must not be used without specific authorisation.

h. attempts or succeeds in obtaining unauthorised access to technology resources, attempts to breach any security measures on any such system, attempts to intercept any electronic transmissions without proper authorisation, or unauthorised use of credentials, including constructing electronic communication so that the communication appears to be from another person/organisation;

i. broadcasts unsolicited personal views contrary to school policy on any matter;

j. fails to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus;

k. involves advertising, political lobbying or the conduct of business for another organisation;

l. propagates chain emails or forwarding messages to groups or School distribution lists without the consent of the user;

m. results in unauthorised external access to the School's technology resources;

n. consumes excessive bandwidth;

o. interferes with the ability of others to conduct the business of the School; or

p. offends or potentially offends the ethos, principles and/or foundations of the School.

Section 85ZE of the Crimes Act 1914 (Cth.) applies to the offensive or harassing use of a telecommunication service, including email, and states that a person shall not knowingly or recklessly:

- use a telecommunications service supplied by a carrier to menace or harass another person; or
- use a telecommunication service supplied by a carrier in such a way as would be regarded by reasonable persons, as being, in all the circumstances, offensive.

Section 57(1) of the Classification (Publications, Films and Computer Games) Enforcement Act 1995 (Vic.) prohibits a person from using an on-line information service to publish or transmit or make available for transmission, objectionable material. An 'on-line information service' is defined to mean "a service which permits, through a communication system, on-line computer access to or transmission of data or computer programs" (s. 56) and is capable of extending to emails.

Section 56 defines 'objectionable material' to mean a publication, film or computer game that;

a. depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that it offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that it should not be classified; or
b. describes or depicts a person who is, or looks like, a minor under 16 engaging in sexual activity or depicted in an indecent sexual manner or context; or
c. promotes, incites or instructs in matters of crime or violence; or
d. is unsuitable for a minor to see or play; or
e. is classified RC or would, if classified, be classified RC (where RC means 'refused classification')."

Section 3 of this Act further defines an 'objectionable publication' to mean a publication that;

> "*lacks serious literary, artistic, political, educational or scientific value and describes, depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in a manner that a reasonable adult would generally regard as unsuitable for minors*."

In addition to sanctions or penalties that may be imposed by the School in relation to prohibited uses, there are legal sanctions for improper use of the technology resources (e.g., sections 247A – 247I of the Crimes Act 1958 (Vic.)).

In the context of the above list, where a message is received that contravenes or potentially contravenes this Policy, that message should be immediately deleted and the sender immediately advised that further inappropriate communications should not be sent.

Where a website is visited inadvertently that contravenes, or potentially contravenes this Policy, that website should be exited immediately.

Once the message has been deleted or the website exited, the user is required to advise The HR Manager and/or the ICT Manager of inadvertent access to inappropriate material and the action taken. This action is required to minimise negative implications for the user.

In cases where there is doubt about the appropriateness of the information being communicated, this matter should be brought to the attention of a member of the Leadership team.

Consequences of Unacceptable and/or Prohibited Use

The School will take disciplinary action against any person found to have engaged in an unacceptable or prohibited use of the School's technology resources. Disciplinary action may include termination of employment.

Employees are advised that unacceptable and/or prohibited use may contravene State and/or Federal legislation. Legal action may be taken against any person in breach of, or allegedly in breach of, these statutes.

Where there is a reasonable belief that illegal activity may have occurred, the School will report the suspected illegal activity to the appropriate authority.

The School reserves the right to remove material causing an undue load on the system.

Computer Viruses/Malware/Ransomware

Electronic and web communications are potential delivery systems for computer viruses/malware/ransomware. All data, programs and files which are downloaded electronically or attached to messages should be scanned by an anti-virus program before being launched, opened or accessed.

Viruses/Malware/ransomware has the potential to seriously damage the technology resources of KDS. Do not open any attachments or click on any links embedded in an email unless you have confidence in the identity of the sender.

Receipt of a message with an unknown or suspicious attachment is to be immediately notified to the KDS ICT Helpdesk.

Monitoring of Electronic Communication

Employees are responsible for regularly checking their received electronic communication to ensure a timely and professional approach is maintained in all School-related communication.

Employees must put an “Out of Office” message on their email with a message indicating the period of absence and who should be contacted in their absence and/or a forwarding of their email to another School-based email address for checking during periods of leave.

The School uses filtering software to restrict access to information and messages which may be in breach of this policy. The possible failure of such software to block such information should not infer any legitimacy or compliance with this policy.

The school uses deep packet inspection technology via is firewall platform to filter traffic for harmful content. A certificate is required to be installed if staff wish to use BYOD devices.

Personal and Financial Information

The King David School will not be liable for any loss incurred by a person, including an employee, who provides personal information, including bank and credit card details via the school’s technology resources.

Data Breach

A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse.

This data breach response plan sets out procedures and clear lines of authority for The King David School staff in the event that the School experiences a data breach (or suspects that a data breach has occurred). If you suspect a data breach has occurred you must inform the Principal as soon as you are aware of a potential concern.

Disclaimer

The King David School makes no warranties of any kind, whether express or implied, in relation to the technology resources.

The School will not be responsible for any damage, including loss of data resulting from delays, non-delivery, etc suffered by any employee using the school’s technology resources.

Use of any information obtained via the Internet is at the employee’s own risk with responsibility for the accuracy or quality of information obtained through its computer network services specifically denied by the School.

RESPONSIBILITY

- Principal
- All King David Staff

RELATED LEGISLATION

- Privacy Act 1988 (Cth) (including the Australian Privacy Principles)
- Copyright Act 1968 (Cth)
- Spam Act 2003 (Cth)
- Crimes Act 1958 (Vic)

RELATED POLICIES

- Child Safety and Wellbeing Policy May 2024
- Respectful Workplace Policy April 2023
- Privacy Policy June 2024
- Social Media Policy April 2023

RELATED DOCUMENTS

- Electronic Communication with Parents Guidelines

NEXT REVIEW

April 2025