KESSER TORAH COLLEGE

Cnr Blake & Napier Streets Dover Heights NSW 2030

02 9301 1111 | info@ktc.nsw.edu.au | www.kessertorah.nsw.edu.au

INFORMATION TECHNOLOGY, COMPUTER AND TELEPHONE CODE OF USE FOR STAFF

INTRODUCTION

Information technology is an essential business tool which makes it possible for the College to operate effectively and efficiently. If it is misused, information technology can damage the College's reputation and viability, cause breaches of the College's legal obligations, and result in legal or financial liabilities and penalties for the College and/or our employees or contractors ('**Staff Members**').

This document sets out the College's information technology, computer and telephone Code of Use ('**Code**'), which applies to the use of all College telephones and computers (including use of the College's network server, software, public network, internet, e-mail, electronic diaries and other electronic communication technologies) which are accessed (including remote access), provided or funded (in whole or in part) by the College, whether kept at the College's premises, your home or some other location ('**College Systems**').

Parts of this Code also apply to your use of computers, mobile telephones and other mobile and wireless devices including tablets and iPads outside College Systems, such as your personal computer or mobile telephone ('**Other Systems**').

The Code does not form part of any contract, including any employment contract. Instead, the Code sets out the rules which must be complied with when using College Systems, and Other Systems in certain circumstances. The Code also explains how and to what extent the College monitors your use of College Systems.

This Code is not intended to be exhaustive, and it does not anticipate every possible use of College Systems. Staff Members are encouraged to act with caution and to take into account the underlying principles of this Code. If you feel unsure about how or whether this Code applies at any time, you should contact the Principal or Chief Executive Officer.

All Staff Members using College Systems must comply with this Code. Departure from compliance with this Code may only be authorised by the Principal or Chief Executive Officer.

This Code may be updated or revised from time to time at the College's discretion. If you are unsure of whether you are using the latest version of this Code, you should contact the Principal, Chief Executive Officer or relevant Coordinator.

Consequences of breach of this Code

The College may hold you responsible (including financially liable) for any:

- damage to College Systems or equipment caused by you;
- costs incurred as a result of you accessing any internet site or sending any electronic message (such as email, sms or voicemail); and/or
- liability of the College to any person created by your use of College Systems or Other Systems.

If a Staff Member acts in a manner which is inconsistent with this Code or in any other inappropriate manner, the College may take disciplinary action. Disciplinary action may include limitation or removal of access to College Systems, or termination of employment/engagement with the College. In some circumstances, the College may also decide to take legal action against a Staff Member, including to recover any costs it incurs as a result of the Staff Member's failure to comply with this Code.

RESPONSIBILITIES OF STAFF

Accountability and care of equipment and software

Staff Members must use College equipment and software carefully, and follow all instructions about how to use it and take care of it.

All College Systems users are issued with a unique username and password. You are solely accountable for all actions performed under your username and password - it is no excuse for you to say that you did not log out of your account and someone else used it. Whenever you leave your computer unattended, you should lock or log off from your computer. You must also follow all other directions from the IT Manager in relation to the security of College Systems.

The College may hold a Staff Member responsible for any:

- damage to College equipment and/or software caused by the Staff Member's use of College Systems and/or Other Systems;
- costs incurred by the Staff Member's access of internet sites; and/or
- legal obligation to any person created by the Staff Member's use of College Systems.

When using internet and electronic communications, Staff Members must:

- always identify themselves clearly and honestly;
- not tell anyone their password or allow any other person to use their College user account, except as required by the College; and
- never access another person's email or internet account without that person's permission or the permission of the College.

If you believe the integrity of your login or password(s) has been compromised, you should contact the IT Manager through Helpdesk so new password(s) can be assigned.

Any Staff Member with a College laptop must bring the laptop to the College on each day that he/she attends the College premises, and perform a manual backup in accordance with the IT Manager's direction.

Viruses

The internet, e-mails and e-mail attachments are potential hosts for computer viruses. The downloading of infected information from the internet and emails is potentially fatal to the College computer network.

Staff members must not knowingly introduce a virus to College Systems.

All external files and attachments must be virus checked using scanning software before they are accessed whether from an email or any form or external media. Virus checking is done automatically

through the 'OfficeScan' software installed on the mail server. In addition, .zip and .exe files are blocked at the Firewall and a return message is sent to the sender regarding any unacceptable attachment. Staff Members must not disable or circumvent these tools, particularly when sending or receiving emails and accessing or downloading information from internet sites.

Staff Members should exercise extreme caution when opening emails and attachments from unknown senders and when downloading any file or information from internet sites. If you are concerned about an e-mail attachment, or believe that it has not been automatically scanned for viruses, you should contact the IT Manager through Helpdesk as soon as possible.

If a Staff Member has remote access or uses mobile computer devices for business purposes, he/she must use approved anti-virus scanning tools when sending and receiving emails (including attachments) and accessing the internet. The College may suspend access if it suspects that viruses are reaching College Systems through a Staff Member's computer (including mobile devices).

Information authenticity and quality

Staff Members must not base any important decisions on information accessed through the internet without first confirming the authenticity and quality of that information.

Student use of College Systems

College students have access to College Systems subject to the College's Guidelines for Student Use of College Computers, the Internet and E-Mail. Staff Members who supervise student use of College Systems must be familiar with these Guidelines and make reasonable efforts to ensure that students comply with the Guidelines.

PERMITTED AND PROHIBITED USES OF COLLEGE SYSTEMS

Permitted uses

College Systems must only be used:

- for College business and educational purposes, except as otherwise set out in this Code; and
- in a professional, appropriate and lawful manner.

Personal and other uses

The College may, as a matter of discretion, allow use of College Systems for other purposes, so long as this does not:

- contravene other parts of this Code;
- in the College's opinion, adversely impact on performance of work duties or the functioning of educational programs; and
- is not, in the College's opinion, unreasonable or excessive, in terms of time, resources and/or additional costs to the College.

For example, as a matter of discretion, the College currently permits limited use of its telephone facilities to make and receive personal calls, and limited use of its internet and e-mail facilities to send and receive personal messages and to perform personal research.

The College may cease to allow such other uses at any time. Excessive use of the telephone, e-mail, or internet facilities for personal reasons may result in disciplinary action, as mentioned above.

Prohibited uses

College Systems must not be used to:

- engage in any activity for personal financial gain;
- send unsolicited commercial or advertising electronic messages (spam) or mass mail, or send or receive chain mail;
- disseminate or store commercial or personal advertisements, viruses, political material or any other unauthorised purpose;
- gamble, wager or bet;
- access or contribute to electronic bulletin boards or social networking sites such as MSN, Facebook and Myspace, other than for educational purposes;
- access inappropriate internet sites; or
- perform any activity using an anonymous or misleading identity.

College Systems or Other Systems must not be used to:

- interfere with the normal operation of College Systems;
- access parts of College Systems you are unauthorised to access;
- compromise the security of College Systems;
- install software or programs (including peer to peer file sharing programs) on College Systems, or connect computer or mobile or wireless devices to College Systems, unless the College has authorised you to do so;
- violate any of the College's software licensing agreements
- injure the reputation, business or viability of the College; or
- defame, discriminate, harass, threaten, vilify or otherwise offend any director, officer or Staff Member of the College or any other person associated with the College - this requirement also applies to your conduct on social networking sites.

College Systems or, if a Staff Member is representing himself/herself in any way as associated or connected with the College, Other Systems, must not be used to:

- transmit, receive, access, download, store, publish and/or create material that is, or could be construed to be: obscene; derogatory; defamatory; harassing; threatening; vilifying; racist; sexist; unlawfully discriminatory; sexually explicit; pornographic; or otherwise offensive to any individual, organisation, association, company or business or their reputation; and/or
- breach any law or engage in any other illegal or inappropriate activity, including the infringement of copyright or other intellectual property rights of another person.

Downloading or installing software

Software (licensed, shareware, freeware, evaluation or otherwise) including system, application or data files may only be downloaded using procedures approved by the Principal, Chief Executive Officer or the IT Manager.

Staff Members must not install any software on College Systems except as approved by the Principal, Chief Executive Officer or the IT Manager. Also, Staff Members not install or use encryption software on College Systems other than that provided by the College without prior authority.

LOGGING AND MONITORING

All actions performed using College Systems are logged and monitored by the College or by another person on the College's behalf. You should expect this monitoring to be continuous and ongoing. This monitoring includes document creation, file management, electronic communications which are sent to or by Staff Members, both internally and externally, telephone and mobile telephone usage (such as numbers called and the length of calls), and their internet activity (including the sites visited, the content of those sites and the time spent at each site). The College may copy, access or disclose any information or file that is stored, processed or transmitted using College Systems.

Staff Members should not have any expectation of privacy for any actions performed using College Systems, including personal e-mails or documents. Staff Members should also be aware that all information and data stored on College Systems may be archived by College management as it considers appropriate. This means that the College may be able to access or retrieve information even if it has been deleted.

The College may access, copy or disclose any information or data stored, processed or transmitted on College Systems, including disclosure to the police or as evidence in legal proceedings.

PREVENTED INTERNET ACCESS OR EMAIL DELIVERY

The College may stop e-mails from entering or leaving its e-mail system if it believes it is appropriate to do so. The College may also block access to internet sites as it considers appropriate.

DEALING WITH E-MAILS

College Property

The College is the owner of copyright over all e-mail messages created by Staff Members as part of their employment/engagement.

Inappropriate messages

You and/or the College may be liable for what you say in an e-mail message, sms or voicemail message). A message that may seem harmless to you may be highly offensive to someone else. The audience of an inappropriate comment in an e-mail may be unexpected and extremely widespread; e-mail is not private. It may easily be copied, forwarded, saved, intercepted, archived and may be subject to discovery in litigation.

In determining whether a message falls within any of the categories of prohibited uses, or is generally inappropriate, the College will consider the response and sensitivities of the recipient of a message rather than the intention of the sender.

If you receive a message which you think may be inappropriate, delete it immediately and do not forward it to anyone else. You should also discourage the sender from sending further materials of that nature. You should also report the incident as soon as possible to the IT Manager through Helpdesk.

Confidentiality and security

When an e-mail is sent from the College to the network server and then on to the internet, the e-mail messagemay become public information. Encryption reduces the risk of third parties being able to

read e-mails. As a result, you should encrypt e-mail messages which contain sensitive information before sending them. If you need more information about encrypting messages, you should contact the IT Manager through Helpdesk.

Items of a highly confidential or sensitive nature should not be sent via e-mail, even with encryption. There is always a trail and a copy saved somewhere, not necessarily only on the College's network server.

On occasion, e-mail may be used to correspond with recipients who are unknown or cannot be identified. You should ensure that you are able to identify the intended recipient, and you should take care when sending or responding to such e-mail messages.

There is also a risk of false attribution of e-mail. Software is widely available by which e-mail messages may be edited or 'doctored' to reflect an erroneous message or sender name. The recipient may as a result be unaware that he or she is communicating with an imposter. Accordingly, you should maintain a reasonable degree of caution regarding the identity of the sender by other means if you have concerns.

E-mail may be truncated, scrambled, delayed, sent to the wrong address or not arrive at all. If outgoing e-mail is important or urgent, you should verify that the recipient has received the e-mail in its entirety.

Representing the College

When Staff Members send e-mail messages for College business purposes or any other purpose connected with the College:

- if they make any representations on behalf of the College, Staff Members must ensure that these representations are checked by a Coordinator, the Chief Executive Officer or the Principal;
- if they are writing to a student or family member about a significant issue - such as discipline, welfareor assessment - then (as with any letter to students or their families) Staff Members must get approval from a Coordinator, the Chief Executive Officer or the Principal before sending the e-mail. Routine communication (eg setting a time for a meeting or confirming when work is due) can be sent without approval; and
- the manner of expression used in the e-mail must be consistent with the relevant business or educational purpose.

Comments that are not appropriate in the workplace or school environment will also be inappropriate when sent by e-mail. As noted above, e-mail messages can easily be misconstrued. Accordingly, words and attached documents should be carefully chosen and expressed in a clear, professional manner.

It is generally expected that:

- teachers will respond to e-mails from students, parents, colleagues or the College Executive within 2 working days; and
- all other staff (administrative and executive) will respond to external e-mails in a timely fashion.

If this is not possible, for whatever reason, you should advise your immediate supervisor and work with him or her to organise a solution to this issue.

Disclaimer

In light of these issues, you must ensure that all e-mails that are sent from your College e-mail address contain the College's standard disclaimer message, which reads as follows:

> *'KTC claims copyright in this email. Our emails are confidential and may contain legally privileged information. You must not copy, transmit, use or disclose any part of this email, or any attachments, without our consent. If you think you have received this email in error, please notify us immediately by return email or on (02) 9301 1111 at our cost, and delete this email.*
>
> *KTC monitors the use of its computer systems, including emails, on a continuous basis. You should not assume that this email is private, even if it is personal in nature.*
>
> *Any opinion expressed in this email is not the opinion of KTC unless it is stated to be so. No person is permitted to conclude any binding agreement on behalf of KTC without written authorisation from the Principal.*
>
> *KTC does not represent or warrant either that the integrity of this email has been maintained, or that the email is free of viruses. We do not accept liability for any loss or damage caused by this email, including through a virus.'*

This message is set to appear automatically on each outgoing e-mail. You must not delete or amend this disclaimer. Please contact the IT Manager through Helpdesk if this feature is not working.

Absences

If you are likely to be absent from work for any lengthy period of time, you should make arrangements for your e-mails to be accessible to the College or ensure that an 'out of office reply' is automatically set. This automatic reply will alert those trying to contact you that you are away from work and that important queries should be directed to a nominated colleague. If you require assistance in activating this feature, please contact the IT Manager through Helpdesk.

Storage

You should delete old or unnecessary e-mail messages and archive those e-mail messages you need to keep. This is because retention of messages fills up large amounts of storage space on the College network server and can slow down performance. If there are items in your e-mail which you require at a later date, please ensure that these are saved in your network directory so that appropriate backups are made by the College.

INTELLECTUAL PROPERTY

When distributing information over College Systems, either internally or to third parties outside the College, you must ensure that you and the College have the right to do so and that you are not violating the intellectual property rights of the College or any third party. This requirement also includes conduct on Other Systems, in relation to College intellectual property and/or if Staff Members are representing themselves in any way as associated or connected with the College.

This obligation applies in the same way when copying information or downloading software.

In particular, copyright law may apply to the information you intend to distribute or copy, and must always be observed. The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files and downloaded information) must not be distributed through e-mail without specific authorisation to do so. This material may be able to be used and copied in a limited way for research or educational purposes.

Staff Members should acknowledge the source of any material they use for any work purpose (including author, title, publisher and internet address) and, where appropriate, obtain the permission of the author or publisher.

If you are unsure whether you are permitted to distribute or copy particular information, you should contact your Coordinator.

PRIVACY

In the course of carrying out your duties as a Staff Member of the College, you may have access to or handle personal information relating to others, including other Staff Members, students, parents, suppliers and contractors.

Staff Members must not access personal information or make it public, disclose it to anybody else, copy or remove it from the College premises or College Systems (in hard copy or electronic form), unless it is necessary for the proper performance of their duties or they are authorised to do so.

E-mail should not be used to disclose personal information of another person, except in accordance with the College's Privacy Policy or with authorisation from the Principal or Chief Executive Officer.

In order to comply with the College's obligations under privacy law, you are encouraged to use the blind copy option when sending e-mails to multiple recipients, because disclosure of those persons' e-mail addresses may impinge upon their privacy.

You are encouraged to familiarise yourself with the National Privacy Principles (**NPPs**) and ensure that your use of e-mail does not breach the Privacy Act 1988 (Cth) or the NPPs. If you have any questions about the Privacy Act and/or the College's obligations, please contact the Principal or Chief Executive Officer.

LOSS OF DATA

The College accepts no liability for the loss of any data that Staff Members store on College Systems, whether or not that data was stored in compliance with this Code.

USE OF COLLEGE SYSTEMS AFTER TERMINATION

On termination of employment, Staff Members access to all College Systems will be terminated. Staff Members should return any telephones, laptops, computers and software in relation to College Systems that they were given access to during their employment/engagement. Staff Members must ensure that no material or software has been improperly copied or amended through the use of College Systems.

USER ACCEPTANCE

Signing the attached acknowledgment and returning it to the Chief Executive Officer indicates that you have read and understood this Code.

……

I have read and understand the College Information Technology, Computer and Telephone Code of Use set out above and will comply with this Code.

_____ _____

Name Date

_____

Signature