East Preston Islamic College

EPIC ICT POLICY

Updated June 2021

1. Purpose

1.1. The purpose of this Policy is to ensure that all use of East Preston Islamic College (EPIC) Information, Communications and Technology (ICT) resources is legal, ethical, and consistent with the aims, values and objectives msv us3(9opeC)-2.7 (8-3.3)10 (,)7.8 (y (s)eC)-2. hatnsillitiuest,

3.5. Large data downloads or transmissions should be minimised to ensure the performance of EPIC ICT resources for other users is not adversely affected. Where a user has caused EPIC to incur costs for excessive downloading of non-work related material in breach of this Policy, EPIC may seek reimbursement or compensation from the user for all or part of these costs.

3.6. E-Mail is to be used for college purposes only and not for personal use.

4. EPIC Property

4.1. Electronic communications created, sent or received using EPIC email systems are the property of EPIC, and may be accessed by an Authorised Person (Principal, Vice Principal, Head of IT) in the case of an investigation, including in relation to investigations following a complaint or investigations into misconduct. Electronic communications may also be subject to discovery in

5.6. If at any time there is a reasonable belief that EPIC ICT resources are being used in breach of this Policy, the Principal/Vice Principal or Head of IT of the person who is suspected of using EPIC ICT resources inappropriately may suspend a person's use of EPIC ICT resources and may require that the equipment being used by the IT Department while the suspected breach is being investigated.

5.7. Nothing in this Policy prevents the EPIC IT Department from monitoring EPIC ICT resources in order to support the functioning and performance of EPIC's information systems.

6. Defamation

6.1. EPIC ICT resources must not be used to send material that defames an individual, organisation, association, company or business. The consequences of a defamatory comment may be severe and give rise to personal and/or EPIC liability. Electronic communications may be easily copied, forwarded, saved, intercepted or archived. The audience of an electronic message may be unexpected and widespread.

7. Copyright

7.1. The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files, music files, video files, text and down loaded information) must not be used without authorisation to do so. The ability to forward and distribute electronic messages and attachments and to share files greatly increases the risk of copyright infringement. Copying material to a hard disk or removable disk, printing or distributing or sharing copyright material by electronic means, may give rise to personal and/or EPIC liability, despite the belief that the use of such material was permitted.

8. Illegal use

8.1. EPIC ICT resources must not be used in any manner contrary to law or likely to contravene the law. Any suspected offender will be referred to the police or other relevant authority and their employment may be terminated.

8.2. Certain inappropriate, unauthorised, and non-work-related use of EPIC ICT resources may constitute a criminal offence under the Crimes Act 1958 (Vic), for example, computer [illegible]

8.4. EPIC is an institution charged with the safety and education of children. Child pornography represents the antithesis of EPIC's responsibilities to children. Any suspected offender will be referred to the police and their employment will be terminated if the allegations are substantiated.

9. Offensive or Inappropriate Material

9.1. Use of EPIC ICT resources must be appropriate to a workplace environment. This includes but is not limited to the content of all electronic communications, whether sent internally or externally.

9.2. EPIC ICT resources must not be used for material that is pornographic, harassing, hateful, racist, sexist, abusive, obscene, discriminatory, offensive, or threatening. This includes sexually oriented messages or images and messages that could constitute sexual harassment.

9.3. Users of EPIC ICT resources who receive unsolicited offensive or inappropriate material electronically should delete it immediately. Offensive or inappropriate material received from people known to the receiver should be deleted immediately and the sender of the material should be asked to refrain from sending such material again. Such material must not be forwarded internally or externally or saved onto EPIC ICT resources except where the material is required for the purposes of investigating a breach of this policy.

10. Social engineering

10.1. Social engineering is (in the context of information security) the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. ICT Acceptable use Policy.

Phishing, Vishing and Whaling and other forms of social engineering are used to obtain information from users that could result in unauthorised access to EPIC ICT resources, or to fraudulently obtain money from the Department.

11. Confidentiality and Privacy

11.1. Electronic communication is not a secure means of communication. While every attempt is made to ensure the security of EPIC ICT resources, users must be aware that this security is not guaranteed, particularly when communicated to an external party. The sender should consider the confidentiality of the material they intend to send when choosing the appropriate means of communication.

11.2. In relation to communications relating to the disclosure of improper conduct either as part of an audit or as contemplated by the Whistleblowers Protection Act 2001 (Vic), it is advised that personal, not EPIC, email accounts or other means of communication are used to report this information to maintain confidentiality.

16. Printing

16.1. Printers in the labs and other common area are intended to serve the individual printing needs of users, not as a replacement for photocopy machines. Users who need to produce multiple copies of a document should print a master copy and then photocopy it. By using photocopy machine

16.2. Any printing problem such as paper jamming or replacing printer cartridge should be reported to local IT administrator, user should not open or try to fix printer.

16.3. All printing is monitored via Papercut. If you no longer have enough credit to print you must report it to the Head of IT.

17. Records Management

17.1. Email messages that are routine or of a short-term facilitative nature should be deleted when reference ceases, as distinct from ongoing business records such as policy or operational records.

17.2. Retention of messages fills up large amounts of storage space on the network and can slow down performance. As few messages as possible should be maintained in a user's mailbox. Messages for archive should be kept in separate archive files stored on the user's network

Territory and covers sexually explicit material that contains real depictions of actual sexual intercourse and other sexual activity between consenting adults.

b. Involves racial or religious vilification.
c. Is unlawfully discriminatory.
d. Is defamatory.
e. Involves sexual harassment; or
f. Brings or has the potential to bring the employee and/or DEECD into disrepute.

19.5. Category 4: Excessive personal use during working hours

This category covers personal use which satisfies the following 3 criteria –

a. it occurs during normal working hours (but excluding the employee's lunch or other official breaks); and
b. it adversely affects, or could reasonably be expected to adversely affect the performance of the employee's duties; and
c. the use is more than insignificant

20. College Data – Conclusion of Employment

All data, email, SharePoint, server and Foldr is property of EPIC. In the event your employment is terminated, or you choose to end your employmen