East Preston Islamic College

EPIC ICT POLICY

Updated July 2019

EPIC ICT POLICY

Contents

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 of EPIC and its responsibilities to the students in its care. It also has occupational health and safety obligations to employees and students and must comply with State and Federal anti-discrimination and sexual harassment laws. It is thus of paramount importance that its ICT resources are used appropriately and professionally at all times.

1.2. EPIC ICT resources must be properly and efficiently used. EPIC ICT resources are not to be used for inappropriate activities for example, pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment, including sexual harassment, stalking, privacy violations and illegal activity, including illegal peer-to-peer file sharing.

1.3. The use of EPIC ICT resources carries with it responsibilities. Users must at all times remember that when using EPIC ICT resources, they are using ICT resources provided to them for business purposes.

1.4. The provision of EPIC ICT resources by EPIC is to improve and enhance learning and teaching and conduct of the business and functions of EPIC. It is essential that use of this valuable resource be managed to ensure that it is used in an appropriate manner.

1.5. The process by which EPIC seeks to manage staff use of EPIC ICT resources is through the development and implementation of this Policy. The Policy must be followed whenever using EPIC ICT resources.

1.6. This Policy applies to all users of DEECD ICT resources regardless of work location and applies to all aspects of use of all DEECD ICT resources, for example:

- *Publishing and browsing on the internet;*
- *Downloading or accessing files from the internet or other electronic sources;*
- *Email;*
- *Electronic news groups /notice boards or blogs*
- *Social networking; File transfer;*
- *File storage;*
- *File sharing;*
- *Video conferencing;*
- *Streaming media;*
- *Instant messaging; Online discussion groups and 'chat' facilities;*
- *Subscriptions to list servers, mailing lists or other like services;*
- *Copying, saving or distributing files;*
- *Viewing material electronically; and*
- *Printing material.*

1.7. Any reference in this Policy to an Act, Regulation, Guidelines, Code of Conduct or other document includes a reference to the Act, Regulation, Guidelines, Code of Conduct or other document as amended from time to time.

2. Non-Compliance

2.1. Depending on the nature of the inappropriate use of EPIC ICT resources, non-compliance with this Policy may constitute:

- *a breach of employment obligations;*
- *serious misconduct;*
- *sexual harassment;*
- *unlawful discrimination;*
- *a criminal offence;*
- *a threat to the security of EPIC ICT resources;*
- *an infringement of the privacy of staff and other persons; or*
- *exposure to legal liability.*

2.2. Non-compliance with this Policy will be regarded as a serious matter and appropriate action, including termination of employment, may be taken.

2.3. Where there is a reasonable belief that illegal activity may have occurred EPIC may report the suspected illegal activity to the police.

3. Business Purposes and Other Use

3.1. Users of EPIC ICT resources may use EPIC ICT resources for personal use provided the use is not excessive and does not breach this Policy. Users must not engage in excessive personal use of EPIC ICT resources during working hours. Users must not engage in excessive personal use of EPIC email systems or the internet using EPIC networks outside working hours. A breach of either of these constitutes a failure to abide by this Policy. In using EPIC ICT resources for personal use, users should be aware that the provisions that apply to access and monitoring of EPIC ICT resources apply to personal use as well.

3.2. Subscribing to mailing lists and other like services using EPIC ICT resources must be for EPIC purposes or professional development reasons only.

3.3. Social networking, on-line conferences, discussion groups or other similar services or tools using EPIC ICT resources must be relevant and used only for EPIC purposes or professional development activities. When using such tools, all EPIC ICT users must conduct themselves professionally and appropriately.

3.4. Provided that use is not unlawful, offensive or otherwise improper, users are allowed reasonable access to electronic communications using EPIC ICT resources to facilitate communication between employees and their representatives, which may include a union, on matters pertaining to the employer/employee relationship.

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 litigation and criminal investigations. All information produced on computer, including emails, may be accessible under the Freedom of Information Act 1982 (Vic). Please note that email messages may be retrieved from back-up systems and organisations, their employees and the authors of electronic communications have been held liable for messages that have been sent.

5. Access and Monitoring

5.1. EPIC ICT resources may be accessed or monitored by Authorised Persons at any time without notice to the user. This includes, but is not limited to, use of EPIC email systems and other electronic documents and records.

5.2. Before accessing or monitoring EPIC email systems, the Head of IT is required to contact the Principal/Vice-Principal to inform him/her of the proposed access.

5.3. Authorised Persons may access or monitor the records of EPIC ICT resources for operational, maintenance, compliance, auditing, legal, security or investigative purposes. For example, electronic communications, sent, received or forwarded using EPIC ICT resources, may be accessed and logs of websites visited using EPIC ICT resources may be generated, examined and monitored.

5.4. Principal/Vice-Principal may require the assistance of the Head of IT to gain access to records held within EPIC ICT resources such as electronic documents, communications or website logs of users. In such cases, the Head of IT will not be in breach of this Policy simply by reason of following the instructions of the Principal/Vice-Principal.

If, at any time, the Head of IT discovers any inappropriate use of DEECD ICT resources, they must report their concerns to the Principal/Vice-Principal.

5.5. Use of EPIC ICT resources constitutes consent to access and monitoring in accordance with this Policy.

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 "hacking" and the distribution of computer viruses.

8.3. Illegal or unlawful use includes but is not limited to use of certain types of pornography (eg child pornography) under the Crimes Act 1958 (Vic), offences under the Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (Vic), defamatory material, material that could constitute racial or religious vilification, unlawfully discriminatory material, stalking, blackmail and threats under the Crimes Act 1958 (Vic), use which breaches copyright laws, fraudulent activity, computer crimes and other computer offences under the Cyber Crime Act 2001 (Cth) or Crimes Act 1958 (Vic) (as amended by the Crimes (Property Damage and Computer Offences) Act 2003 (Vic)), or any other relevant legislation.

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 Whistle-blowers 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.

11.3. EPIC will handle any personal information collected through the use of EPIC ICT resources in accordance with the Information Privacy Act 2000 (Vic).

11.4. EPIC will not disclose the content of electronic communications created, sent or received using EPIC ICT resources to third parties outside of EPIC unless that disclosure is required for the purposes of an EPIC investigation, a police investigation or for other legal, investigative, audit or compliance reasons or in other circumstances where that disclosure does not contravene the Information Privacy Act 2000 (Vic).

12. Surveillance and security

12.1. The College has the capability to monitor the use of the College's information technology systems. Staff and students must recognize that whilst the College is committed to maintaining the privacy of personal information, it may be necessary for the College to monitor electronic communications (including email records) in order to comply with applicable laws, or if its suspects there has been a breach of this policy, or to determine ownership or the recipient of lost or misdirected files.

12.2. Users must comply with the College's requirements issued from time to time with respect to the use of encryption or secure transmission channels for particular categories of content.

12.3. Users must not allow access to a site on a College intranet or extranet to a third party if access is blocked to such third parties.

12.4. Users should not do anything which would or might lead to circumventing or compromising security of any of the College's information technology systems.

12.5. The following requirements apply to users in respect of security and system integrity:

- The College's corporate IT policy: password security must be complied with at all times
- ITS rules of use

12.6. All network access should be authenticated through the Microsoft Active Directory (AD).

12.7. Standard usernames and email addresses should be used and the password policy complied with at all times.

12.8. Unauthorized use of another user's account or viewing of their personal files is prohibited.

If identical email addresses will result use of other letters to differentiate between the addresses will be used.

13. Virus/Malware

13.1. Electronic and web communications are potential delivery systems for computer malware. 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.

13.2. Virus/Malware has the potential to seriously damage EPIC ICT resources. Do not open any attachments or click on any links embedded in an email unless you have confidence in the identity of the sender.

14. Attribution

14.1. There is always a risk of false attribution of breaches of this Policy. It is possible that communications may be modified to reflect a false message, sender or recipient. In these instances, an individual may be unaware that he or she is communicating with an impostor or receiving fraudulent information. If a user has a concern with the contents of a message received or the identity of the publisher of the electronic information, action should be taken to verify their identity by other means. If a user believes an electronic communication has been intercepted or modified, the line manager or principal should be informed.

14.2. Users are accountable for all use of EPIC ICT resources that have been made available to them or leased to them for work purposes and all use of EPIC ICT resources performed with their UserID. Users must maintain full supervision and physical control of EPIC ICT resources, including notebook computers, at all times. UserIDs and passwords must be kept secure and confidential. Users must not allow or facilitate unauthorised access to EPIC ICT resources through the disclosure or sharing of passwords or other information designed for security purposes.

14.3. Active sessions are to be terminated when access is no longer required, and computers secured by password when not in use.

15. Mass Distribution and 'SPAM'

15.1. The use of EPIC ICT resources for sending 'junk mail', for-profit messages, or chain letters is strictly prohibited.

15.2. Mass electronic communications should only be sent in accordance with normal EPIC procedures.

15.3. The use of electronic communications for sending unsolicited commercial electronic messages ('Spam') is strictly prohibited and may constitute a breach of the Spam Act 2003 (Cth).

16. Printing

16.1. Printers in the labs and other common area are intended to serve the individual-copy 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 home or shared drive.

18. Complaints

It is expected that any complaint will, in the first instance, be made to the college.
A formal complaint may be made by visiting the college and completing the Complaint, Grievances and Concerns forms located at the administration office.
As a general rule, it should be directed to:

- The Vice Principal, where there are issues relating to staff members or complex student issues or
- The Principal, if there are issues relating to college policy or college management, or if earlier attempts at resolution have been unsuccessful.

If you are unsure of who to contact, the Vice Principal will assist.

Complainants should be aware even though the Vice Principal and Principal are happy to meet with you, please make an appointment to ensure that you are not disappointed if they are not available, and that you do not waste your time by coming to the school.

EPIC may investigate complaints arising from the use of EPIC ICT resources.

19. Breaches of this Policy

19.1. Breaches of this Policy may be categorised using the following categories. The categories do not cover all breaches of this Policy, for example the categories do not specifically refer to breaches of copyright. Matters not covered by the following categories will be dealt with on an individual basis and on the relevant facts.

19.2. Category 1: Illegal

This category covers the following:

a. Child pornography – offences relating to child pornography are covered by the Crimes Act 1958 (Vic) and the Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (Vic). Child pornography is defined in section 67A of the Crimes Act 1958 (Vic) as: "a film, photograph, publication or computer game that describes or depicts a person who is, or appears to be, a minor engaging in sexual activity or depicted in an indecent sexual manner or context."

b. Objectionable material – offences relating to the exhibition, sale and other illegal acts relating to "objectionable films" and "objectionable publications" are covered by the Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (Vic). Such material has or would attract a classification of X18+ (restricted) or RC (refused classification) under the Guidelines for Classification of Films and Computer Games 2005 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth).

c. Any other material or activity which involves or is in furtherance of a breach of the criminal law.

19.3. Category 2: Extreme

This category involves non-criminal use of material that has or would attract a classification of RC under the Guidelines for Classification of Films and Computer Games 2005 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth). This covers any material 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 they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should not be classified;

b. describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether or not the person is engaged in sexual activity or not); or

c. promotes, incites or instructs in matters of crime or violence.

19.4. Category 3: Critical

This category involves other types of offensive material. This covers any material that: 10 Acceptable use policy

a. Has or would attract a classification of X18+ under Guidelines for Classification of Films and Computer Games 2005 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth). The material covered by this classification is only available for hire or sale in the ACT and Northern

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.