Community Radio
Shop 6 Bowling Arcade, Colac
Post: P.O. Box 31, Colac 3250
Ph: 0352 321 991
Email: admin@ocrfm.org.au
Web: www.ocrfm.org.au
ABN 35 575 865 292

OCR FM COMPUTER USE POLICY

AIM

This policy is for IT Systems and all of OCR FM's computer equipment and is designed to protect OCR FM, our members, customers and other visitors from harm caused by the misuse of our IT systems, data and equipment. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime. It can also be the misuse of the internet, downloading illegal data, unwanted programs and general disregard of Station requirements.

Everyone who works at OCR FM is responsible for the security of our IT systems and the data on them, plus the care and handling of the equipment. As such, all members must ensure they adhere to the guidelines in this policy at all times. Should any member be unclear on the policy or how it impacts their role they should speak to the responsible Director or the Board Of Management.

DEFINITIONS

The following definitions apply:
"Users" are everyone who has access to any of OCR FM's IT systems and equipment. This includes all members and also visitors, contractors, agencies, consultants, suppliers, customers and the like.

"Systems" means all IT equipment that connects to the OCRFM network or access station applications. This includes, but is not limited to, desktop computers, laptops, smart phones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

POLICY

This policy covers only internal use of OCRFM's systems. Some aspects of this policy affect areas governed by local legislation in certain countries (e.g., employee privacy laws): in such cases the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases local teams should develop and issue users with a clarification of how the policy applies locally. All members at OCRFM who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

Use of IT Systems

All data stored on OCR FM's systems is the property of OCR FM. Users should be aware that the station cannot guarantee the confidentiality of information stored on any OCR FM system except where required to do so by local laws.
OCR FM's systems exist to support and enable the station to successfully broadcast and undertake general station business. A small amount of personal use is, in most cases, allowed. However it must not be in any way detrimental to users own or their colleagues productivity and nor should it result in any direct costs being borne by OCR FM other than for trivial amounts (e.g., an occasional short telephone call).

Community Radio
Shop 6 Bowling Arcade, Colac
Post: P.O. Box 31, Colac 3250
Ph: 0352 321 991
Email: admin@ocrfm.org.au
Web: www.ocrfm.org.au
ABN 35 575 865 292

OCR FM trusts the members to be fair and sensible when judging what constitutes an acceptable level of personal use of the station's IT systems. If members are uncertain they should consult the Board Of Management.

Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorised access is prevented (or at least made extremely difficult). However this must be done in a way that does not prevent – or risk preventing – legitimate access by all properly-authorized parties.

OCR FM can monitor the use of its IT systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the email and data files of any user, and examination of the access history of any users.

OCR FM reserves the right to regularly audit networks and systems to ensure compliance with this policy.

Data Security
If data on OCR FM's systems is classified as confidential this should be clearly indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorized access to confidential information. Users are expected to exercise reasonable personal judgment when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise transfer to a non-OCR FM system any information that is designated as confidential, or that they should reasonably regard as being confidential to OCR FM, except where explicitly authorized to do so in the performance of their regular duties.

Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with OCR FM's safe password policy.

Users who are supplied with equipment by OCR FM are responsible for the safety and care of that equipment, and the security of software and data stored it and on other OCR FM systems that they can access remotely using it.

Because information on portable devices, such as laptops, tablets and smart phones, is especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

Users who have been charged with the management of OCR FM's systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, root kits, worms, backdoors) being imported into OCR FM's systems by whatever means and must report any actual or suspected malware infection immediately.

Unacceptable Use
All volunteers should use their own judgment regarding what is unacceptable use of OCR FM's systems. The activities below are provided as examples of unacceptable use, however it is not exhaustive. Should

Community Radio
Shop 6 Bowling Arcade, Colac
Post: P.O. Box 31, Colac 3250
Ph: 0352 321 991
Email: admin@ocrfm.org.au
Web: www.ocrfm.org.au
ABN 35 575 865 292

a member need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from the Station Executive before proceeding.

- All illegal activities. These include:
  - theft,
  - computer hacking,
  - malware distribution,
  - contravening copyrights and patents, and
  - using illegal or unlicensed software or services.
  - These also include activities that contravene data protection regulations.

- All activities detrimental to the success of OCR FM. These include:
  - sharing sensitive information outside the company,
    - ✓ such as research and development information, and
    - ✓ customer lists (e.g.: passing on of phone numbers etc),
    - ✓ as well as defamation of the station and its members.

- All activities for personal benefit only that have a negative impact on the day-to-day functioning of the station. These include activities that slow down the computer network (e.g., streaming video, playing networked video games).

- All activities that are inappropriate for OCR FM to be associated with and/or are detrimental to the stations's reputation. This includes:
  - pornography,
  - gambling,
  - inciting hate,
  - bullying and harassment.

- Circumventing the IT security systems and protocols which OCRFM has put in place.

Enforcement

OCR FM will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. While each situation will be judged on a case-by-case basis, members should be aware that consequences may include the termination of their involvement/membership with OCR FM.

Use of any of OCR FM's resources for any illegal activity will usually be grounds for summary dismissal, and OCR FM will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

This policy was adopted as policy in principle by the OCR FM Committee of Management

Signed *Tyson Graham* Date 15th September 2021

This Policy is due for review within 18 months of the date shown above.