JORVIK RADIO
ACCEPTABLE USE POLICY
VERSION 1.2 - UPDATED 08.11.2023

Purpose
The purpose of this Policy is to establish acceptable practices regarding the use of Jorvik Radio's Information Resources in order to protect the confidentiality, integrity and availability of information created, collected, and maintained.

Scope
This policy applies to the use of Jorvik Radio's systems, credentials, and equipment by employees, volunteers, suppliers, or any other person working with Jorvik Radio.

This Policy covers use of all of Jorvik Radio's IT resources, including:

- services, such as email, telephony services, voice over internet protocol ('VOIP') and wireless telephony, voice mail, databases, internet/intranet access; and
- equipment, such as workstations, portable computing devices (including but not limited to mobile devices such as mobile phones or tablets), servers and associated infrastructure and peripheral equipment such as disk drives, portable storage devices, printers, and photocopiers.

This policy helps to ensure individuals operate in a manner which is ethical and lawful under applicable regulation and legislation, including:

- Data Protection Act 2018 ('DPA');
- EU General Data Protection Regulation 2016 ('GDPR');
- Privacy and Electronic Communications Regulation 2003 ('PECR');
- Copyright, Designs and Patents Act 1988;
- Computer Misuse Act 1990; and
- Any subsequent legislation that supersedes the above.

Responsibility
All individuals are responsible and accountable for compliance with this policy and must read and understand it, and all other Jorvik Radio policies.

Anyone that becomes aware of activity that breaches this policy should report it immediately to the Head of IT, Station Manager, or designated Safeguarding Officer as appropriate.

Acceptable Usage

Individuals **must not**:

- view, edit, share, transfer or undertake any other processing of Jorvik Radio data without the appropriate authority to do so.
- use for any purpose which is illegal, against statutory law, unethical, against Jorvik Radio policy or that could offend, intimidate, harass, or upset others including viewing, downloading, copying, sending, or posting material such as pornographic, defamatory, libellous information or pictures.
- publish in any form anything that will bring Jorvik Radio or its partners reputation into dispute.
- raise funds for or promote political candidates, parties, or views.
- store or distribute digital media such as music, film, eBooks, or photographs where Jorvik Radio does not have the right to do so.
- use Trademarked and/or Copyrighted software or content without prior permission or licence.
- download or install any software onto any Jorvik Radio equipment - only Jorvik Radio's Technical Support Team are permitted to do so.
- enter into any electronic transactions that may bind the Company unless appropriately authorised.
- send emails and attachments containing personal or sensitive data unless encryption is employed. The Technical Support Team can provide advice on how to do this.
- access another person's personal accounts, including email, WebVT, and Slack, regardless as to whether their permission was given to do so.
- upload or attempt to upload material to Jorvik Radio's systems via any channel other than those officially provided to an individual. This includes using another individual's upload link.
- tamper with or attempt to damage any property, including systems used for broadcasting, security, resilience, and support.
- use non-approved methods of communication for company business.
- use non-standard communications platforms to discuss personal or sensitive data unless end-to-end encryption is enabled.
- use portable storage (for example USB drives) unless approved by the Head of IT.
- load unauthorised software, including games and freeware.
- allow any family members or friends to use Jorvik Radio devices, systems, or credentials for any reason.
- post content containing Jorvik Radio's branding in any environment that does not abide by Jorvik Radio's brand guidelines, or that suggests it is 'official' where this has not been approved by the Operations Team.
- use Jorvik Radio credentials for non-business purposes, including signing up to non-authorised/non-pertinent services.

- impersonate or pose as a representative of Jorvik Radio where not authorised to do so, including accessing or otherwise interacting with official Jorvik Radio accounts or attempting to misrepresent an individual's responsibilities within the organisation.
- interfere with any settings, controls, or permissions that could impact the organisation's output, security, or quality.
- connect any device directly or via VPN to Jorvik Radio's network. This includes laptops, desktops, mobile phones, or any other network device.
- activate automatic forwarding of email outside of Jorvik Radio systems unless authorised by the Technical Support Team.
- plug in any device to a LAN port associated with Jorvik Radio's network without approval from the Head of IT.
- bring any form of liquid, including drinks or cleaning materials, within proximity of technical equipment unless expressly permitted.
- plug in any device to sockets where the device has not been suitably PAT tested.
- change any content linking to Jorvik Radio accounts without approval from the Head of IT, including email signatures, online bios, and other website content.
- amend any password for accounts belonging to Jorvik Radio, including social media, user accounts, hardware, and networks.
- forward or 'chain' viral or spam content to or from a Jorvik Radio account.
- use Jorvik Radio's systems, space, or network to create inappropriate or illegal content.
- operate in a malicious or negligent manner in spaces owned or operated by Jorvik Radio, including outside events, where harm or damage may occur.

Individuals **must**:

- take care when opening incoming emails and e-mail attachments which are from an unknown source or raise any suspicions due to unusual message headings or form of content. These should always be treated as suspicious as they may contain a virus infection. If in doubt, seek guidance from Jorvik Radio's Technical Support Team prior to opening. Do not forward the email.
- ensure that, whilst limited personal use of email and the internet is acceptable, that this use does not extend to activities required outside of those necessary to fulfil their duties on behalf of Jorvik Radio.
- only connect approved devices to the Jorvik Radio IT infrastructure. This includes mass storage devices, memory sticks, and other approved mobile data devices.
- ensure any device that connects to, or attempts to connect to, Jorvik Radio's network (for example, the studio Wi-Fi) runs the latest version(s) of any software/operating system and abides by the rules outlined within this policy.
- be aware of the effect their social media communications may have on both their own and Jorvik Radio's image and reputation. Individuals are responsible for ensuring that any 'posts', 'tweets' or other communication made on social media sites (including in personal time) are appropriate.

Enforcement

Use of Jorvik Radio's IT systems will be monitored to detect and prevent misuse, including remote access and security cameras (installed in the interests of health, safety and security as per Jorvik Radio's Lone Working obligations) which retain recordings for a period of up to 30 days. Individuals using resources (including the equipment or space protected by Jorvik Radio's monitoring) for personal use cannot assume a right to personal privacy or confidentiality. This includes the contents of email or IM messages.

Jorvik Radio does not wish to examine personal information but reserves the right to monitor any activity on any Jorvik Radio technology resource, to the extent permitted by applicable law. Jorvik Radio will not proactively monitor the content of electronic communications or internet usage unless there is reasonable cause to do so.

Jorvik Radio's Technical Support Team will periodically monitor applications installed on corporate devices and reserve the right to delete any applications or content that were installed without suitable authorisation.

Unreasonable or inappropriate use may be subject to removal of access to systems and disciplinary action up to and including suspension or termination.

FORMAL ATTESTATION

I HAVE READ AND UNDERSTOOD THIS DOCUMENT IN ITS ENTIRETY AND AGREE TO THE CONTENT AND PRINCIPLES LISTED HEREWITHIN:

NAME: _____ DATE: _____ SIGNATURE: _____