HMIPS
HM INSPECTORATE OF PRISONS FOR SCOTLAND
INSPECTING AND MONITORING

Acceptable Use Policy HMIPS-CMS

Document Details

Version	Version 1.0
Issue Date	21 February 2024
Review Date	21 February 2024
Document Approver	Wendy Sinclair-Gieben, HM Chief Inspector of Prisons for Scotland (HMCIPS)
Document Author/ Owner	Graeme Neill, Operations Manager

Version history

Version Date	Reason for release/ version update	Issued by

Document approval

Name	Job Role	Date approved
Wendy Sinclair-Gieben	HMCIPS	21 February 2024

CONTENTS

1. Introduction and purpose

1.1 HMIPS are responsible for all information created relating to the prison monitoring process by Independent Prison Monitors (IPMs) and HMIPS staff. This includes all information generated using the HMIPS-CMS system now and in the future and Rota Management and Training records applications, provided for in the HMIPS-CMS system. For personal data and sensitive personal data held within these systems, HMIPS is the Data Controller and has a legal obligation to ensure that it is maintained securely at all times. Users must be vigilant when using IT equipment or mobile devices to access the HMIPS-CMS system.

1.2 This Acceptable Use Policy has been produced to protect HMIPS and its partners from harm caused by the misuse of our Information Technology (IT) systems and information. It defines the ways in which HMIPS online systems must be used, identifies the key risks of misuse, and informs users of their responsibilities.

Please note that acceptable use of the SCOTS network, used by HMIPS staff and IPMs is defined in the Scottish Government IT Code of Conduct A copy of this document should be provided to IPMs by HMIPS staff if required.

1.3 The policy forms part of HMIPS wider Information Governance Policy Framework, which includes HMIPS-CMS Terms and Conditions of use, HMIPS Data Protection Policy, Managing Information Security Incidents and Records Management Policy.

1.4 For the purposes of this policy:

- Users relates to IPMs and HMIPS staff.
- Systems relates to HMIPS – CMS.
- Device relates to all IT equipment (except SCOTS IT equipment) used to gain access to HMIPS – CMS (including but not limited to: mobile phones, laptops, desktop computers, iPads and tablets).

1.5 All information held within HMIPS – CMS has been provided to support you in your role. This information should not be shared with anyone outside of the organisation without authorisation. This includes sharing electronically (soft copy), printed copies, information on social networking sites, publication online, verbally and printed media.

2. Unacceptable use

2.1 Unacceptable use is defined by HMIPS as any action which contravenes or potentially contravenes any statutory, regulatory or legislative obligation by which HMIPS is bound, including the data protection law and other information legislation, the Human Rights Act 1998 and the Computer Misuse Act 1990. It is also any action which contravenes the policies and procedures laid down by HMIPS.

2.2 Unacceptable use can also be defined as any action which puts any individual, IPM or a member of HMIPS staff at risk. The activities below are provided as

examples of unacceptable use; however this list is not exhaustive. Should you need to contravene these guidelines in order to perform your role, you should obtain approval from HMIPS and their Senior Information Risk Owner (SIRO) before proceeding.

2.3 Examples of unacceptable use include but are not limited to:

- Theft of IT equipment
- Hacking into IT systems
- Contravening copyrights and patents
- Procuring or selling personal data
- Using illegal or unlicensed software or services on HMIPS systems
- Breaching data protection legislation
- Sharing or disclosing sensitive information outside the organisation
- Creating or sending content that is deemed to be offensive, obscene or indecent
- Sending or posting discriminatory, harassing, or threatening messages or images
- Introducing malicious software onto HMIPS systems
- Sending or posting chain letters or advertisements not related to HMIPS purposes or activities, or on behalf of HMIPS without its knowledge
- Passing off personal views as representing those of HMIPS
- Creating or sending material which is designed to cause annoyance or anxiety
- Corrupting or destroying other user's data
- Violating the privacy of others online
- Contravenes HMIPS Standards and values

3. User IDs and passwords

3.1 The use of another individual's User ID and password is not permitted under any circumstances. You must not disclose your passwords and must take all reasonable precautions to ensure that your password remains confidential. If you disclose your password to someone else you may be held responsible for any improper actions committed under that User ID and accountability may fall equally on you as the holder of the account, as on the individual using the account at the time.

4. Use of personal, mobile and removable devices

4.1 Personal and mobile devices can be remotely connected to the HMIPS- CMS system, but the user is personally liable for their device and content. These devices are especially vulnerable and so it is essential that you adhere to the following rules in order to protect the integrity of information and ensure it remains safe and secure:

- Devices must be locked with a PIN/password
- PINs and passwords must be kept confidential and not shared with anyone else
- Devices should automatically activate their PIN/password after a maximum of 5 minutes of inactivity

- You must inform HMIPS immediately in the event of loss or theft of a device which holds HMIPS information. HMIPS can discuss with you and review the HMIPS information that may be at risk and may wish to exercise the right to take actions to permanently delete this information from the device.
- It is a requirement of use that you adhere to this Acceptable Use Policy.
- OFFICIAL-SENSITIVE, confidential and personal data must not be saved/stored on any mobile personal device out with the HMIPS-CMS system.

4.2 Removable devices include, but are not restricted to the following:

- CDs/DVDs
- External hard drives
- USB memory sticks
- Media card readers
- Embedded microchips (including smart cards and mobile phone SIM cards)
- Digital cameras
- Audio tapes

4.3 There are a number of risks associated with the use of removable devices, including the disclosure of sensitive, confidential or personal data as a consequence of loss, theft or careless use; contamination of networks or equipment through the introduction of viruses. These may result in potential sanctions against HMIPS or individuals imposed by the UK Information Commissioner's Office (ICO); potential legal action against HMIPS or individuals; and potential reputational and financial damage.

4.4 Removable devices must not be used by IPMs or HMIPS staff for the storage and transfer of information relating to HMIPS or its normal business.

5. Before you post any comments or information

5.1 Please consider the following:

- Your name and role will be posted automatically - no posts can be made anonymously
- Please don't say anything that you wouldn't say in person
- Please ensure your comments:
    - Are appropriate and relevant - please don't use forums and blogs to complain about issues which should be addressed via your PMC or the official complaints procedure. Some topics will undoubtedly arouse strong emotion, so please consider your comment before posting it
    - Do not provoke or offend others
    - Are not racist, sexist, homophobic, abusive or otherwise objectionable
    - Do not contain language or a tone that are likely to offend others
    - Are not considered an attack on others, including other IPMs or HMIPS staff

- Do not break the law, such as potentially libellous or defamatory postings, or those in potential breach of copyright are accurate and not likely to mislead others
- Respect other people's opinions and are courteous to all other users

5.2 If you find a comment offensive you should contact your PMC outlining your concerns. If you think a comment is wrong or inaccurate you should contact the individual directly or post up a factual correction.

6. Use of IT and communications equipment

6.1 IT and communications equipment, including laptops and mobile phones, may be provided to you in order to support you in your role. If you are provided with equipment, you must follow the guidelines below:

- Equipment must only be used for the purpose of carrying out your role, personal use of SPS/HMIPS provided equipment is not permitted
- PINs and passwords must be kept confidential and not shared with anyone else
- You must inform HMIPS in the event of loss or theft of a device which holds HMIPS information immediately
- OFFICIAL-SENSITIVE, confidential and personal data must not be transferred and saved/stored on any mobile personal device out with use of the HMIPS-CMs system

7. Use of the internet

7.1 IPM or a member of HMIPS staff should refer to the SG IT Code of Conduct for guidance on the acceptable use of the internet when using SPS computers or SCOTS WiFi

8. Breach of this policy

8.1 All users have a responsibility to adhere to this policy. If a user is found to have used HMIPS IT facilities or information in a way that would be deemed unacceptable, access may be suspended, pending an investigation. For IPMs and HMIPS staff a serious breach of this policy may lead to disciplinary action and dismissal, in accordance with the Staff/Volunteer Code of Conduct. A serious breach of the policy by IPMs and HMIPS staff may lead to investigation by The Standards Commission for Scotland in line with the HMIPS Code of Conduct. Breaches of this policy by IPMs and HMIPS staff may result in the member being removed.

8.2 Further to this, the Computer Misuse Act 1990 identifies three criminal offences of computer misuse, including unauthorised access to computer material, unauthorised access with intent to commit or facilitate further offences and unauthorised modification of computer material. Penalties for breaches of this Act

can be severe, ranging from a fine to five years in prison. It is important that users understand that a breach of this policy and this Act may lead to a criminal investigation and they will be personally liable for any fines or penalties imposed, as a result of the breach.

8.3 Users should report any suspected or known breaches of this policy to HMIPS immediately. Please refer to HMIPS Managing Information Security Incidents Procedure for further information.

8.4 In using HMIPS IT facilities and services each user agrees that HMIPS shall have no liability for the loss or corruption of any user file or files, information or data; and/or the loss or damage to any user owned equipment, devices, systems or other assets resulting from the inappropriate use or misuse of the IT infrastructure.

9. Monitoring and review

9.1 HMIPS will monitor the use of its IT systems and the information held on its systems, on a regular basis. Compliance with this policy will be monitored by the HMIPS Senior Information Risk Owner (SIRO) and regular audits of networks and systems may be undertaken. HMIPS acknowledge that it will be necessary to play a proactive part in identifying, monitoring and managing risks to information as new ways of accessing and using information are developed in the future. The policy will be periodically reviewed in order to take account of any new or changed legislation, regulations or business practices, or use of new technology.