HMIPS
HM INSPECTORATE OF PRISONS FOR SCOTLAND
INSPECTING AND MONITORING

Volunteers Code of Connection

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

Introduction

HM Chief Inspector of Prisons for Scotland assumes overall responsibility for prison monitoring. This is carried out on a day to day basis by independent prison monitors (IPMs). The role holds statutory authority under the Public Services Reform (Inspection and Monitoring of Prisons) (Scotland) Order 2015. IPMs provide an independent viewpoint on the humane treatment and conditions for prisoners in all prisons across Scotland and conduct investigations raised by prisoners. Monitors report formally on their findings. The HMIPS-CMS system forms part of the reporting process. This statement details the Terms and Conditions of service use for all HMIPS – CMS system users.

Terms and Conditions

1. I will ensure that I comply with data protection legislation, including the General Data Protection Regulation (GDPR), privacy and information security legislation.

2. I will ensure that I comply with the information handling requirements established by HMIPS, using only the HMIPS-CMS to document and communicate HMIPS business.

3. I will seek to prevent inadvertent disclosure of sensitive or classified information by ensuring that I work in appropriate locations, to avoid being overlooked, that I do not leave my devices unattended when logged into the HMIPS-CMS system and that I show appropriate care if uploading or printing any documents from the system.

4. I agree to protect access to the system by only using my authorised login credentials and a password to access it.

5. I will not share my login credentials with anyone and understand that I may be held liable for any compromise or abuse of the credentials where I have not protected them appropriately.

6. I will report any actual or suspected disclosure of my login credentials to HMIPS staff without delay.

7. I will not use any other user's credentials to gain access to the HMIPS-CMS system.

8. When communicating on HMIPS business, I will only use my authorised HMIPS email account and I commit to not forwarding or sharing sensitive information via the HMIPS-CMS system with external parties unless authorised to do by HMIPS staff.

9. I confirm that I will keep my devices' security software up to date for the purposes of using the HMIPS-CMS system. Furthermore, I understand that the security

settings on the devices should be in keeping with the requirements set out in the Acceptable Use Policy.

10. I recognise that it is best practice to regularly apply operating system updates and security patches to the system used to access the HMIPS-CMS system and I will not attempt to bypass or subvert system security controls or use them for any purpose other than intended.

11. I confirm awareness that HMIPS has the right to monitor my use of the system, in line with the Acceptable Use Policy, and may require access to any messages for the purposes of audit, investigation, and compliance with legislation.

12. I understand that, when accessing HMIPS-CMS my location data will be used to confirm that I am accessing them from within the UK. If I turn off or deny access to location data, I will be denied entry to the system.

13. I understand that HMIPS reserves the right to restrict or terminate my connection to the HMIPS-CMS or aspects of it if I am found to be operating inappropriately, my conduct or activity is putting the security of the system at risk. Similarly, I recognise that if remedial action is identified for me and no progress is demonstrated in line with HMIPS requirements, my access to the HMIPS-CMS may be terminated.

14. In the event of a security or data breach I commit to inform HMIPS without undue delay, in line with the Managing Information Security Incidents Policy. I understand that HMIPS reserve the right to investigate security incidents and confirm that, if an investigation is necessary, I will provide full support to the best of my ability.

15. In accepting these terms and conditions, I am acknowledging and confirming I have read, accept and follow the following policies:

- Acceptable Use Policy
- Data Protection Policy
- Managing Information Security Incidents Policy

16. When you use the chat facility you should be aware of your responsibilities as you create, add and share:

16.1 Any content created or shared within chat is subject to the HMIPS-CMS Managing Information Security Incidents Policy, HMIPS-CMS Acceptable Use Policy and the SG IT Code of Conduct Policy (Your PMC can provide you with these documents if required).

16.2. Do not share the personal information of prisoners or users, including names. All chat content is subject to Freedom of Information rules.

16.3. A 30 day deletion policy is in place to protect users and to meet Data Protection laws.

16.4. The chat facility should not be used to make business decisions that are important to the organisation and would therefore qualify as “Corporate value”. If it is identified that this has happened then a PMC should be advised and the information will be extracted, assigned a corporate value marker and stored securely within the SG Records Management System (eRDM). Doing so will ensure you fulfil your responsibility to ensure the organisation is able to retain the history and evidence of our day-to-day business activities and key decisions as part of that corporate record. This serves as a primary source of the truth and keeps us compliant with key legislation such as the Public Record Scotland Act 2011.