




Information Matters

Reporting a Data Breach


Staff that identify a data loss, become aware of or suspect a data loss or a near miss, must immediately (within one hour) notify **HMPPS Information Security (InfoSec) & Services** team via the reporting line and bring it to the attention of the designated responsible manager, or in their absence, another manager.

 **0203 334 0324**

Data Loss Reporting Line – Save it in your work phone!

Working remotely

When working remotely all staff must have read the following guidance:

 **Use of Information Security & Information Technology for HMPPS Staff Remote working & using personal IT devices**



Line Managers should retain evidence of the staff member for assurance purposes.

Handling Personal Data

Emailing of HMPPS information must be by secure email, do not use a private email address.

Before  **SENDING** please  **DOUBLE CHECK** the recipients of your email.

HMPPS information should be stored only on approved IT infrastructure

 **Please ensure that you do not discuss sensitive issues in public spaces** 

Clear Desk

All staff are responsible for adhering to the Clear Desk policy and ensure that HMPPS information is not left unattended, or on desks in the sight of others without a need to know.

When periodically away from your desk, at the end of a working day, or when leaving a meeting room ensure that you remove any information from the unattended space and lock computers using Ctrl-Alt-Del.

Digital 1st First st

Hey there!

Let's make
Probation Service
GREENER

And let's protect
INFORMATION SECURITY

Please only print when
absolutely necessary
GO DIGITAL FIRST

Finding InfoSec online

To find HMPPS Information Security information on the HMPPS Intranet pages navigate to the following:

SUPPORT
|
INFORMATION SECURITY (INFOSEC)
|
GUIDANCE