Ministry of Justice

HM Prison & Probation Service

Policy Name: Information Security Policy Framework

Reference: N/A

Re-Issue Date: 26 May 2023 **Implementation Date**: 29 January 2020

Replaces the following documents which are hereby cancelled:

- PSI 24 /2014 - AI 18/2014 - PI 18/2014

Action required by:

☒	HMPPS HQ	☒	Governors
☒	Public Sector Prisons	☒	Heads of Group
☒	Contracted Prisons	☒	Contract Managers in Probation Trusts
☒	Probation Service	☒	Under 18 Young Offender Institutions
☒	HMPPS Rehabilitation Contract Services Team	☒	HMPPS-run Immigration Removal Centres (IRCs)
☒	Other providers of Probation and Community Services		

Mandatory Actions: All groups referenced above must adhere to the Requirements section of this Policy Framework, which contains all mandatory actions.

For Information: All information asset owners, information asset custodians, senior managers, delivery partners and third-party suppliers.

Governors must ensure that any new local policies that they develop because of this Policy Framework are compliant with relevant legislation, including the Public-Sector Equality Duty (Equality Act, 2010).

How will this Policy Framework be audited or monitored:

Mandatory elements of instructions must be subject to management checks (and may be subject to self or peer audit by operational line management/contract managers/HQ managers, as judged to be appropriate by the managers with responsibility for delivery. In addition, HMPPS will have a corporate audit programme that will audit against mandatory requirements to an extent and at a frequency determined from time to time through the appropriate governance.

Resource Impact:
All Public-Sector Prisons, Probation Service divisions, Contracted Prisons, Headquarters Groups, and third-party suppliers must have an information asset register in place which must be reviewed on a quarterly basis and documented as being done for audit purposes.

All Public-Sector prisons, Probation Service divisions, contracted prisons, headquarters groups, and third-party suppliers must have an information risk register in place which must be reviewed on a quarterly basis and documented as being complete for audit purposes.

The Information Asset Owner is responsible for ensuring that all their staff complete information assurance training when they start their employment with HMPPS and that they complete refresher training at regular intervals thereafter.

Contact: informationmgmtsecurity@justice.gov.uk

Deputy/Group Director sign-off: Adrian Scott, Executive Director; Change, Strategy and Planning Directorate

Approved by OPS for publication: Sonia Crozier and Michelle Jarman-Howe, Joint Chairs, Operational Policy Sub-board, November 2022.

Revisions

Date	Changes
14 November 2022	Addition of para 3.17 and Annexes C, D and E, in relation to Peer Support Workers
23 November 2022	Removal of references to CRCs and Bent Faxes (now decommissioned)
26 May 2023	Para 3.3 has a minor amendment

CONTENTS

1. Purpose

Information Security is the practice of managing risks related to the use, processing, storage, and transmission of information or data. It is also ensuring the systems and processes used for those purposes are in line with the organisational policies.

- Information is the lifeblood of our organisation, it is a critical business asset that HMPPS needs to protect and get the most value from to benefit the business.

- It is important that only authorised sources have access to HMPPS information, at the right time and the correct details

2. Outcomes

This policy sets out HMPPS commitment to ensuring that adequate security controls operate effectively on our information (whether held electronically or in hard copy). It also sets out what prison establishments, the Probation Service, headquarters groups, their 'delivery partners' and third-party suppliers and providers of contracted prison and probation services should do to maintain adequate controls on HMPPS information. In doing so, this policy supports the HMPPS strategic aims and objectives and should enable employees throughout the organisation to identify their roles and responsibilities in handling HMPPS information.

3. Requirements

3.1 Information Assurance

"Information requiring protection" and "Protected information" are terms that are used throughout the rest of the policy to describe information that if lost or in some form compromised, would have a degree of impact to either individuals or the organisation.

Information must be valued throughout its lifecycle to ensure the maintenance of accurate and current records, with clear review, retention and disposal policies in line with relevant legal and regulatory frameworks.

Personal information - that of offenders / prisoners, staff, and anyone else that we may hold personally identifiable information on - will always require a baseline level of protection.

We must control and appropriately protect our information assets throughout the entire lifecycle – from initial creation of the information, through its use and the purpose it fulfils in the organisation, to final disposal / destruction.

Physical security measures must be used to deny unauthorised individuals' access to assets including protectively marked material e.g. Assets where the Probation Service & Other Third Sector Agencies are co-located.

3.2 Data Protection Act 2018

The Data Protection Act (2018) is UK legislation which we must comply with when processing personal information.

The core principles of the Data Protection Act 2018, which we must comply with, are:

- used fairly, lawfully and transparently
- used for specified, explicit purposes

- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

3.3 Information Asset Owners (IAO)

All Prison establishments, Probation Service (PS) and headquarters groups must identify an Information Asset Owner for
their information assets and they must be senior individuals involved in running the relevant business. In establishments these are Governing Governors, Probation Service these are Deputy Directors of Probation and at HQ are Directors.

Information Asset Owners must follow the rules for dealing with information assets laid down by statute (including The UK General Data Protection Regulation (UK GDPR), The Data Protection Act 2018, the Human Rights Act 1998) as well as the minimum mandatory measures contained within this guidance.

Information Asset Owners must escalate substantial risks and issues through the HMPPS Information Security (InfoSec) & Services team InformationmgmtSecurity@Justice.gov.uk or by telephone on 0203 334 0324. These will be escalated to the HMPPS SIRO if they cannot be resolved or guidance provided.

3.4 Information Asset Register

An Information Asset register must exist for every public prison establishment, PS Division, HQ Directorate, and contracted prison.

A local Information Asset Register template, supplied and supported by the HMPPS Information Security (InfoSec) & Services Team, must be maintained and reviewed on a quarterly basis. Evidence of the quarterly review should be captured, for example, recorded in minutes of a senior management team meeting, but also within the register itself.

Information asset registers must record the following about your information:

- details about staff and contractors accessing your information assets
- transfers of information and the use of removable media
- the security classification of the information asset
- the retention period depending on class of asset

All information assets must be recorded on the register, regardless of format, classification, purpose, or age. Whilst realistically it may be difficult to account for every single piece of information asset, any identified asset should not be excluded from the register.

Assets with the classification of SECRET or TOP SECRET must not be recorded on an Information Asset Register. This information must be recorded and looked after as per the instructions for this classification of information as made available to authorised staff on a need to know basis.

3.5 Information Risk Register

To provide evidence that the risks in their business area have been identified and that there are plans in place for managing them the IAO must compile and maintain an Information Risk Register.

IAOs must review information risks on a quarterly basis as part of the review of the establishment / business group/company information asset register and, where appropriate, escalate any risks to the HMPPS Information Security (InfoSec) & Services Team at InformationmgmtSecurity@Justice.gov.uk or by telephone on 0203 334 0324. As well as existing risks that have already been identified, the review must also consider forthcoming potential changes in services, technology and threats.

3.6 Privacy Notice

The Privacy Notice for Prisoners / Offenders must be displayed in print for viewing at the earliest possible opportunity, for example, Reception in prison establishments', and reception areas of probation offices being used by all providers of probation services.

The Notice for Prisoner Visitors must be displayed in print for viewing in the reception / waiting area and in the visits centre.

The Notice for staff in prisons with Traka key management system must be displayed in the Traka cabinet room (Traka is a biometric key dispensing system).

3.7 Compliance Statement

In order to confirm that the requirements of this policy are being met, HMPPS functions will be required to complete and return an annual statement of compliance. A template will be provided via the Senior Leaders Bulletin.

3.8 Information Assurance Training

The information Asset Owner is responsible for ensuring that all their staff complete information assurance training when they start their employment with HMPPS and that they complete refresher training at least once per year thereafter. Approved e-learning is hosted on Civil Service Learning. The HMPPS Information Security (InfoSec) & Services Team are also responsible for the annual refresher training across HMPPS.

3.9 The Government Security Classification Scheme

All information assets in the Ministry of Justice, of which HMPPS is an Agency, must have an associated classification, as defined by Government Security Classification Scheme.

The existence of a protective marking might help to make a decision about access, but every case must be considered on its own merits.

All information assets in HMPPS must be classified using the Government Security Classification (GSC) see PSI 12/2014 Government Security Classification.

From the publication of this policy, new documents created by HMPPS must be risk assessed for sensitivity and appropriately marked. File covers should be marked with the highest level classification of any of the contents (documents classed as Official need not be marked as such).

3.10 Clear desk

A ‘clear desk’ arrangement must be in force in all locations where HMPPS data is held, including sites where co-location is taking place

Staff must ensure that information is not left unattended, or on desks in the sight of others not entitled to see the information (e.g. cleaners, or even colleagues without a need to know’), or left in meeting rooms after meetings have ended, or left in post rooms without being in sealed envelopes.

Staff must adhere to the following standards in relation to the Clear Desk requirement:

- Staff must take a responsible attitude to the protection of HMPPS information during temporary periods away from their work stations in consideration of the HMPPS information accessible, its classification, the length of time the staff member will be away from the workstation and the level of risk the location presents in respect of unauthorised disclosure and / or misuse. For the avoidance of any doubt staff shall remove all HMPPS information from their work area and store it in a locked container or other suitable device at the end of each working day; and / or when the information is no longer required; and / or when the work area is to be vacated.

- Managers must carry out periodic visual checks that desks are cleared and information requiring protection is locked away.

- Staff must ensure the confidentiality of personal information and other organisational information when third parties are present, such as offenders, cleaners, maintenance engineers and visitors from partnership agencies. Personal information that can be viewed on computer screens, paper documents, white boards or charts, must be concealed when third parties are present in the office or when working outside of a secure area.

- Staff must lock their workstations (like using Ctrl/Alt/Del) whenever they move away from the desk.

- Line managers must be informed of any circumstances in which such standards of confidentiality cannot and have not been maintained.

- All information shall be appropriately protected from unauthorised disclosure to any unauthorised user who does not have a legitimate business need to process or view the particular information.

- Any member of staff who cannot comply with this policy due to a lack of suitable lockable storage devices should report this to his / her line manager immediately.

- Any member of staff who observes information left unattended or otherwise in breach of this policy should report this to his / her line manager as soon as possible.

- Information requiring protection must be locked away when not in use.

3.11 Handling information assets outside the office

(For Contracted Service Providers such as private prisons this instruction applies to data that HMPPS shares for the management of offenders and their rehabilitation)

Documents (electronic or paper) classified as OFFICIAL-SENSITIVE and above can be taken out of the office only:

- when they are required for reference at a meeting
- when permission is given (by the IAO or delegated authority) for a staff member to work on the documents away from the office

For all information taken out of the office that requires additional protections, an audit trail must be kept by signing the documents out of the office and back into the office.

Documents containing the personal information of staff or offenders must not be stored on personally owned IT or removable storage devices.

The practice of taking protected information out of the office is in general to be discouraged. Where the work of HMPPS cannot be conducted efficiently unless information is removed from the office, the following rules must be applied:

- Consider whether other methods or options exist to avoid removing the information out of the office
- Can the information be reduced? Only take what is absolutely necessary

Before a staff member can be authorised to remove sensitive documents, the authorising manager must be satisfied that staff are in possession of facilities to protect the document appropriately whilst away from the office, for example, lockable cases.

All HMPPS information must be protected outside the workplace.

3.12 Bulk Movement of data

All bulk movements of electronic information must be authorised by the Information Asset Owner and the HMPPS Information Security (InfoSec) & Services Team.

3.13 Transmitting information

The transmission of information assets is inevitable in order to meet business needs. However, when authorising the movement of information assets between sites you must ensure steps are taken to ensure safe movement of the information and checks are in place to confirm the transfer of the information and the receipt of information.

Transmission by hand

Messengers must carry envelopes between premises in securely fastened or lockable mail bags, pouches or similar containers. They must be given clear instructions about delivering in the absence of the addressee or his authorised representative.

Transmission by E-Mail

Secure means should be used to communicate information requiring protection. The Internet is not a secure medium, therefore protected information must not be sent over the Internet unless a HMPPS authorised method is used.

OFFICIAL (including OFFICIAL SENSITIVE) information must only be sent to addresses with a secure departmental email system. For full details of secure email destinations please refer to PSI 25/2014 PI 19/2014 AI 19/2014 IT Security policy.

Documents marked SECRET and TOP SECRET must not be stored on systems or emailed by systems that are not approved (accredited) for such a level.

Transmission by Telephone (Voice)

Information classified as OFFICIAL-SENSITIVE must not be discussed over the telephone except in extraordinary circumstances. In these circumstances a guarded manner must be used (such as by referring to "the subject of my minute dated yesterday" or "the matter we are both currently engaged upon").

Transmission by Fax

Where there is a high business need and where alternative communication mechanisms are not available, protected information may also be sent. The following protocol must be used:

- If a fax has never been sent to the number before, verify the number by sending a test fax. Confirm with the destination that the test was successful before proceeding further
- If you will likely use the fax number on a regular basis, set up the number as a 'speed dial' on the fax machine. This will help prevent misdialling each time the number is used. Test once programmed in
- If the fax contains sensitive information ensure the recipient is standing by the receiving fax machine waiting for transmission and that promptly confirm the fax has been received correctly and in total

Transmission by Postal Services

Information requiring protection must consider the need for using tracked services such as Royal Mail Recorded and Special Delivery, or delivery by trusted hand, e.g. approved couriers, or staff who are going to the same destination as the material. Sending collated personal information, such as a completed form or full Offender file must always require a delivery receipt.

If sending protected information somewhere where it may be opened in a post room or by a correspondence clerk, then double enveloping is appropriate. In addition to this:

- The inner envelope would bear authorised recipient details and any particular handling requirements to inform the post room how to handle it such as "to be opened by addressee only"
- The outermost cover must bear no indication of the classification or sensitivity of the contents.
- The full forwarding address and a return address (in case of failed delivery) must be given on both the outermost cover and on any inner cover.
- This address must include the name of the official sending the document, and not just "The Governor", "Deputy Director of Probation" or "Head of Group".
- This is to ensure that, should the document be returned, it is not opened by staff that should not have access to the content of the document.
- It is the responsibility of the official who seals the outer envelope to supply the sending address details, and to write on the outer cover what method of delivery is to be used.

Track and trace services must be used for personal / sensitive information.

Tracking of bulk and / or sensitive paper information sent by post or courier

Where bulk and / or sensitive information needs to be sent via postal or courier services a system of audit must be built in to track delivery and provide early warning of any loss or compromise, whether actual or attempted. This can be achieved by sending individual files or small numbers of them jointly via a courier, such as DX, or by Recorded or Special delivery. It should be borne in mind that the tracking service provided by Recorded Delivery is fairly limited, as it only provides a signature on receipt.

Special Delivery is more expensive but offers a more comprehensive tracking service. The sender will have to assess the impact of compromise and judge what level of postal service is appropriate. The carefully sealed or fastened packaging (container, packet, bag or envelope) containing the information must bear a full forwarding address and a return address (in case of failed delivery). A tracking reference number must be obtained. After 48hrs the sender must then check with the intended recipient that the item has been received. If it has not been received then the sender should track its progress using the reference number issued when it was sent. Staff should retain tracking data until there is clear evidence that the item has been received by the intended recipient.

3.14 Information Sharing

Where it is necessary for establishments, Probation Service (PS), and headquarters groups to consult organisations or individuals outside of the public-sector, consideration must be given to the protection of any information assets. Release of information must be strictly on a need-to-know basis.
Information assets sent to organisations that do not operate the Government Security Classification (GSC) scheme (normally private or commercial) may be at risk because the receiving organisation does not understand the meaning or requirements of classifications and associated controls. In these instances, specific handling requirements (in accordance with HMPPS handing controls defined in Policies) must be agreed with the receiving organisation. An Information Sharing Agreement must be considered as per the Information Sharing Policy before any information is sent, which will include the required information security handling instructions.

If a receiving organisation is not capable of securing information assets with the security controls appropriate to its classification or sensitivity, then we [HMPPS] must not transmit the information assets, and must advise the receiving organisation that, until the security control deficiencies are remedied, no transmission will take place.

3.15 Destruction and disposal of information assets

All information that is no longer required for business purposes must be destroyed in an approved manner as per PSI 04/2018 PI 02/2018 AI 03/2018 Records, Information Management and Retention Policy.

For information classified as Secret and Top Secret, destruction must be witnessed by an authorised officer. Governors, Directors of Contracted Prisons, Deputy Directors of Probation, Heads of Groups and Information Asset Owners must ensure that Senior Management Teams and Information Asset Custodians review and are aware of this Policy.

For protected paper information requiring destruction, staff must use either a HMPPS-approved 'confidential waste' contractor or cross-cut shredder equipment approved to government standards.

For all forms of destruction, a receipt or certificate of destruction must be provided by the contractor and retained.

Waste bags containing un-shredded protected information must not be left unsecured, all waste bags containing unshredded information are required to be sealed and kept in a secure, locked storage facility whilst it awaits secure disposal. At no time should Prisoners or People on Probation be left unattended with or have access to confidential waste.

3.16 Information Loss/Compromise Incidents

Staff that identify a data loss, become aware of or suspect a data loss, must immediately (within one hour) notify the HMPPS Information Security (InfoSec) & Services team via the reporting line number (0203 334 0324) and bring it to the attention of the designated responsible manager, or in their absence, another Manager. Delays in identifying incidents may lead to vital information being forgotten or lost.

Any events of information loss or compromise must be reported in accordance with the process in **Annex B**.

3.17 Prisoner Peer Support Workers

In many prison establishments it is common practice to have prisoners working in some form of Peer Mentoring role. This may be in the form of Peer Support Workers, Prisoner Information Desks (PIDs), Prisoner Advice Service (PAS), or Induction & Pre-release Orderlies. This list is not exhaustive as they may have many different variations of the job title.

In order to ensure that prisons that employ prisoners in this type of role are complaint with the DPA & UK GDPR these prisoners will be required to sign a Non-disclosure Agreement **(Annex C).** This explains the consequences of breaching confidentiality and must be read and signed by all Peer Support Workers and Peer Mentors before commencing their employment within this role, with a note made on P-NOMIS case notes of this agreement

All Prison Induction Packs should include a copy of the HMPPS Privacy Notice. A copy of this is available on the Infosec Support page in both English & Welsh. Additionally, we now require the attached paragraph **(Annex D)** to be included in all establishments where Peer Support Workers and Peer Mentors are used.

This paragraph will advise all new reception prisoners that trained prisoners working as Peer Support Workers & Mentors are among those that we may share their personal data with in order to assist them. This paragraph will also advise them that If they do not wish for us to share their personal Information in this way they have a right to do so under UK General Data Protection Regulations (UK GDPR) (Article 15-21), and they should make staff aware at the earliest opportunity, ensuring that all applications are placed in a sealed envelope and marked for “Confidential - Staff only to process”.
Establishments will need to have clear procedures in place to accommodate this.

Whilst job descriptions will vary from role to role and each establishment, certain elements should be included within all job descriptions for any prisoner employed as a Peer Support Worker or Peer Mentor **(Annex E).**
This job description formalises the previous annexes as well as levels of engagement and required training for the role.
Please note the type and level of qualification will differ between different establishments and training providers.

4. Guidance

4.1 Information Assurance

Information is a key organisational asset and employees should consider themselves 'trusted Stewards' of all information with an obligation to protect it.

Information that would cause no impact if it was compromised or lost does not require protections beyond its typical operational/business handling. An example of this is information that is intended or relevant for the public domain – like that published on the Government website or what could be obtained from other public sources.

The Information lifecycle stages are considered as:

- Creating
- Controlling & Storing
- Transmitting & Transporting (both electronic and physical)
- Retention & Archiving
- Disposal & Destruction

What do we mean by 'information'?

Common examples of information in HMPPS include:

- Personal information such as names, addresses, offending history, individual case files
- Policy documents
- Commercial information e.g. contracts or documents pertaining to third party organisations
- Sensitive information, for example relating to security matters, staff disciplinary or investigations

Information can exist in many formats. It could be the contents of: a phone call or email, paper document, file or notebook; audio or video recording; computer, laptop or removable media such as a memory stick or CD.

What is an 'information asset'?

An asset is something that holds value. All information has value and serves purpose to the organisation. If information serves no purpose, consider whether we should be in possession of it. To determine the level of value, consider the following questions:

- How useful is it?
- Will it cost money to reacquire?
- Would there be legal, reputation or financial repercussions if you couldn't produce it on request?
- Would it have an effect on operational efficiency if you could not access it easily?
- Would there be consequences of not having it?
- Is there a risk associated with the information?

- Is there a risk of losing it? A risk that it is not accurate?
- A risk that someone may try to tamper with it?
- A risk arising from inappropriate disclosure?
- Does the group of information have a specific content?
- Do you understand what it is and what it is for?
- Does it include the entire context associated with the information?
- Does the information have a manageable lifecycle?
- Were all the components created for a common purpose?

What is Information Assurance?

Information Assurance is the practice of managing risks related to the use, processing, storage, and transmission of information or data. It is also ensuring the systems and processes used for those purposes are in line with the organisational policies.

Reliable and accurate information is critical to proper decision making in HMPPS. This makes information a vital business asset that we need to protect. Information risk management provides this protection by managing risks to the Confidentiality, Integrity and Availability (CIA) of information to assist our business to function effectively.

- 'Confidentiality' means making sure that information is protected from theft or unauthorised access, make sure that information is not lost or unintentionally revealed.
- 'Integrity' means making sure that we can trust information, that it is accurate and up to date.
- 'Availability' means making sure that the right information is available when and where we need it.

What drives Information Assurance?

Two primary drivers of Information Assurance are legislation and regulations.

Data Protection Act 2018

Failure to comply with requirements of DPA can result in enforcement by the Information Commissioners Office, which may include a monetary penalty of up to 20 Million Euros per incident. DPA legislation underpins much of the policies on Information Assurance, Information Management and Information Security.

Further details of the Data Protection Act and the Freedom of Information Act, their application within HMPPS, and roles & responsibilities of staff, please refer to PSI 03/2018 PI 03/2018 AI 02/2018 - The DPA 2018 and UK GDPR, The FOI Act 2000, EIR 2004

The threats to our information assets

There are a number of basic threats to information assets. The greatest actual risk to information is loss occurring when material is moved outside of secure premises (i.e. sent to other premises, HQ, third parties or for disposal). Other threats are unauthorised access, leaks, electronic attack and malware (viruses).

When losses or compromises occur, apart from any other detrimental consequences, they reflect badly on both the organisation and on the general integrity of the Civil Service. Managers must ensure that all staff are aware of their responsibilities in this context and the

importance of strict adherence to the regulations when dealing with protectively marked information.

Protective measures surrounding our assets

Protective measures fall into three types - personnel security, physical security and IT controls. The aim of personnel security is to ensure that everyone given authorised access to our assets (people, property and information) is trustworthy. Physical security measures are used to deny unauthorised individuals access to assets including protectively marked material. IT security controls are described in PSI 25/2014 PI 19/2014 AI 19/2014 IT Security, such as access authorisation, use of passwords, firewalls and other hardware and software to prevent electronic attacks, encryption, and use of the protective marking system to guide the required level of control

4.2 Roles and Responsibilities and Compliance

Managing information assets across HMPPS is achieved through defined roles and tools. We are required to evidence our management of information assets through 'compliance' activities. Other providers of probation services and contractors, third party suppliers and delivery partners will be required to have information security roles and responsibilities in place in order to comply with legislation and may choose to adopt the roles and responsibilities set out below.

Roles and Responsibilities

HMPPS Senior Information Risk Owner (SIRO)

The HMPPS SIRO has overall responsibility for all HMPPS information assets which are held or owned by HMPPS. The HMPPS SIRO sits on the MoJ SIRO Board and provides assurance that all Information Asset Owners in HMPPS are following their responsibilities. The SIRO is familiar with information risks and would lead the HMPPS response in the event of a major data incident.

Information Asset Owner (IAO)

Information Asset Owners are Governing Governors, Deputy Directors of Probation or HQ Directors but may be other senior managers involved in running the relevant business area. They are responsible for the day to day use as well as the risk management of their information asset and supporting the HMPPS SIRO in carrying out their duties.

The Information Asset Owner is responsible for the creation, use, storage and sharing of the Information Assets for which they have been identified as the owner. They must understand what information is held, what is added, removed and who has access and why. They should use their knowledge to address risks to their Information Assets and ensure the Information Assets are fully used within the law and for the public good.

The Information Asset Owner for each asset (electronic or paper-based and items such as identity cards, DVDs and video tapes) should agree the general protective marking of standard documents/information and the appropriate arrangements to access the information.

The IAO should also be aware of the overarching obligations imposed by the Official Secrets Acts and the Freedom of Information Act 2000.
Detailed guidance for Information Asset Owners can be found in the Information Asset Owner Reference Guidance on the Information Security (Infosec) & Services - Information Assurance page of the HMPPS Intranet.

The IAO may wish to appoint Information Asset Custodians to work on their behalf, taking day to day oversight of assets and reporting back to the IAO on the changes to risks on at least a quarterly basis.

Information Asset Custodians (IAC)

Information Asset Custodians are involved in the day to day use and management of information assets in a particular area, they will be appointed by the IAO to have responsibility for overseeing and implementing the necessary safeguards to protect the information assets and report back to the IAO on any changes to risks. The IAO will retain the overall responsibility.

Information Asset Custodians can be assigned where the business function contains a broad range of information assets or is geographically dispersed. Acceptable uses of the IAC role are:

- Assigned to Head of Functions within Prison establishments (an example where broad range of assets will exist under the control of an IAO).
- Probation Service senior managers, like Heads of LDU Clusters assigned to Controllers of Private Prisons (an example where the IAO sits in a HMPPS HQ function with responsibility for Controller offices that are geographically dispersed).
- Other managerial roles with a local presence governed by a HMPPS HQ Directorate, for example HR or Estates.

Local Information Manager (LIM)

The Local Information Manager (LIM) role is enforced in PSI 04/2018 PI 02/2018 AI 03/2018 Records, Information Management and Retention Policy and takes a lead role in specifically the archiving of information, its length of retention, and the destruction of information once it's no longer required. The LIM should be supported by a Deputy LIM.

The HMPPS Information Security (InfoSec) & Services Team

The HMPPS Information Security (InfoSec) & Services Team is a central function in HMPPS HQ. The team aims to provide information risk management to deliver business benefits and efficiency savings, reduce information risk and facilitate compliance with information legislation.

The team's role is to enable, monitor and develop Information Assurance Maturity and Compliance within HMPPS and contracted service providers. The team also owns and maintains the HMPPS Information Risk Register and provides written advice to the HMPPS SIRO on the security and use of HMPPS assets.

Tools for Managing Information

Providers of probation services and other contractors, third party suppliers and delivery partners will be required to have tools in place for managing information in order to comply with legislation and may choose to adopt the key controls set out below. Where the instruction in italics refers specifically to a contractor or third party supplier they are required to comply with this mandatory instruction, which may be in addition to required actions in ISO 27001.

Information Asset Register

An Information Asset Register is as the name implies – a register of information assets.

It is owned by the Information Asset Owner (see Roles above) but is likely maintained through supporting roles such as Information Asset Custodians, Local Information Managers and similar.

Registers should be created and maintained using an approved template provided by the HMPPS Information Security (InfoSec) & Services Team. The approved template will prompt on the necessary information associated with an asset.

Where required, more detailed audit trails should be kept to mitigate any risks that you may perceive as an information asset owner.

Information Risk Register

Reliable and accurate information is critical to proper decision making in HMPPS. This makes information a vital business asset that we need to protect. Information risk management provides this protection by managing risks to the confidentiality, integrity and availability (CIA) of information to assist our business to function effectively.

A well-organised and easy to understand information risk register is fundamentally important. The register needs to provide enough information to the IAO to enable them to be able to identify and explain the risk management decisions within each business group.

PSI 06/2016 / AI 08/2016 / PI 08/2016 Information Risk Management provides detailed guidance on the risk management process and a template for an Information Risk Register as an annex to the policy.

The HMPPS SIRO defines the level of risk ‘appetite’ for the organisation. Please see document held on the Information Assurance page of the HMPPS Intranet.

Privacy Notice

In support of the first principle of the Data Protection Act, HMPPS is committed to communicating with individuals on the way in which we process personal information by displaying a Privacy Notice. This notice outlines the purposes for which we intend to process personal information.

A copy of the notices can be obtained from the Information Security (Infosec) & Services team at Informationmgmtsecurity@Justice.gov.uk or from the teams support web pages on the

HMPPS Intranet.
Departmental Security Health Check (DSHC)

HMPPS functions may be required to supply information to support the annual requirement of the Departmental Health Check – a requirement of the Cabinet Office.

4.3 Managing and storing information assets

The Government Security Classification Scheme

The requirement to use protective marking on information assets is defined in the PSI 12/2014 / AI 10/2014 / PI 04/2014 HMPPS Government Security Classification Policy, which contains full guidance on how to apply the correct classification and handling controls.

New GSC classifications indicate the sensitivity of information in terms of the likely impact resulting from compromise, loss or misuse, and the need to defend against a broad profile of applicable threats. The classification system has three levels: OFFICIAL, SECRET and TOP SECRET.

OFFICIAL	SECRET	TOP SECRET
The majority of information that is created / processed by HMPPS. Includes routine business operations, including offender and staff personal information, and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.	Very sensitive information that justifies heightened protective measures to defend against determined / highly capability threats. Where compromise may seriously damage military capabilities, international relations or the investigation of serious organised crime.	HMG's most sensitive information requiring the highest levels of protection from the most serious threats. Where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

The security classifications do not have any direct implications for access to information under either the Data Protection Act (2018) or the Freedom of Information Act (2000). Further guidance on these two acts can be found in PSI 03/2018 PI 03/2018 AI 02/2018 - The DPA 2018 and UK GDPR, The FOI Act 2000, EIR 2004 If information has a marking, this does not mean that it is exempt from being disclosed, and if information does not have a marking, this does not mean that it can be automatically disclosed.

The OFFICIAL classification will apply to the vast majority of HMPPS information including:

- general HMPPS activity (finance, estates, personnel, policy, commercial).
- most front-line service operations.

- organisation and performance management information.
- personal information (including staff data, offender case files, citizen data) and
- policy documents.

The classification reflects the fact that reasonable measures need to be taken to look after it and to comply with relevant legislation such as the Data Protection Act, Freedom of Information Act and Public Records Acts.

OFFICIAL information does not require a protective marking

A limited amount of information will be particularly sensitive but will still come within OFFICIAL if it is not subject to the threat sources for which SECRET is designed, even if its loss or compromise could have severely damaging consequences. This information can be described as OFFICIAL SENSITIVE and the need to know principle must be rigorously enforced for particularly where it may be being shared outside of a routine or well understood business process.

There will be very few activities where all related information or cases require the OFFICIAL SENSITIVE marking, though this may apply to assets previously marked as CONFIDENTIAL. Examples include:

- Where there is a specific risk assessment, or threat to highly vulnerable individuals.
- Cases involving intimidation, corruption or fraud.
- Where there is a legal requirement for anonymity.
- Where there is a high media profile and risk of damaging unauthorised disclosure.
- Highly sensitive change proposals or contentious negotiations.
- Major security or contingency planning details.

This more sensitive information must be identified by being marked 'OFFICIAL SENSITIVE'. This marking alerts users to the enhanced level of risk and that additional controls are required.

Key Controls for Creating, handling, storing and transmitting information assets

Before creating information consider the principles of Confidentiality, Integrity and Availability. For example, in deciding whether the information will be paper-based or an electronic file, consider how you will protect it to only those that are authorised or need to know, and how you will ensure the information remains accurate and prevent against mistakes or corruption.

At the time of creation, determine the classification of the information (in accordance with the GSC) if it has not already been defined.

Detailed guidance on how to manage assets can be found in PSI 12/2014 PI 04/2014 AI 10/2014 - Government Secure Classification (GSC) policy.

Controlling access to information assets

A key factor in protecting your information is ensuring that it is only accessed by organisations and individuals who have a business need to access it. By limiting the access to the information, you limit the overall exposure and reduce the risk of compromise.

However, you need to ensure that you do not restrict access unnecessarily, preventing MoJ users from undertaking their legitimate business. Getting the right balance is an important aspect of information assurance for all Information Asset Owners to consider.

For electronic information assets, ensure that appropriate access controls are in place. This may take the form of 'permissions' or role-based access.

For paper and other formats, ensure that physical security controls are in place. For example, consider building and room access control, the use of storage units, where keys are kept and how key access is managed.

Clear desk

You should think carefully about leaving papers unattended on your desk as you would about leaving your own personal correspondence – or even a purse or wallet – in plain view. This means:

- not leaving documents, files or any other information lying around on your desk when you are not using them,
- locking them away in secure storage when you leave the office, and
- not having sensitive information on notice boards displayed in areas accessed by those that do not have a 'need to know', including escorted visitors e.g. central office spaces, staff rest rooms, individual offices.

It would be a mistake to assume that information held even within secure buildings cannot be compromised.

If in any doubt as to the appropriate use and protection of information staff should seek advice from their line manager in the first instance.

Handling information assets outside the office

Guidance on how to manage information away from the workplace can be found in the HMPPS Mobile Computing and Remote Working Guide.

Bulk Movement of information

Bulk movement of information can cover both paper-based information and electronic information. For electronic, consideration is needed as to the volume of data. For example, one physical hard disk being moved may contain multiple (unlimited) individual records.

As the volume of information increases, so potentially does the impact, and therefore the risk rating. As such, bulk movement of information requires a specific risk assessment.

Bulk movements can only take place under exceptional circumstances, for example, during organisational change like a closing premises, or change of ownership.

A Data Movement Form (DMF) is to be used (available from the HMPPS Information Security (InfoSec) & Services Team), and the advice of the HMPPS accreditor is to be sought who may decide to raise with the HMPPS SIRO for approval if the risk is considered in their opinion high enough.

Transmitting information

It is the responsibility of the Information Asset Owner to ensure that the information is received in a safe and secure manner.

Details and guidance on the different methods of transmitting information and how to use them can be found in **Annex A** of this policy.

Information Sharing

Sharing data can result in tangible benefits through improving the way we deliver services and ensuring partner organisations have the data that they need to support HMPPS. However, sharing data can create risks. It is important that we assess these risks and manage them effectively. In some cases, a Data Sharing Agreement will be required. This is a tool which assists with Data Protection Act 2018 compliance and also provides a clear record of the basis, purpose and conditions of the share which is important to ensure these aspects are understood between all the parties.

Details of information sharing and the requirements of a sharing agreement are contained in the Information Sharing Policy Framework.

4.4 Retaining & archiving information assets

Archiving information is the act of storing information once it no longer serves an active purpose. The most common examples of this are:

- Where an Offender in the community completes their Community Order and is no longer required to maintain contact
- Where a Prisoner is released from custody and is no longer held within a Prison environment
- Where a staff member terminates their employment with the organization
- Where a financial transaction is complete

It is typical practice to archive information away from the operational environment (for example, a dedicated room) in order to preserve the information for the required length of time with the right environmental conditions and security controls.

Retaining information is defined by the period of time (length of time) which we are required to store that information. The requirements typically derive from legislation and regulations, but also, are defined by business need and justification.

An archive storage units or dedicated room would likely hold bulk (i.e. large volumes) of information. Protective controls must continue the 'need to know' principle. It would be expected that access to archived information would be limited to select roles.

The HMPPS requirement for the archiving, retention and disposal of information is contained in PSI 04/2018 PI 02/2018 AI 03/2018 Records, Information Management and Retention Policy.

4.5 Destruction and disposal of information assets

In order to satisfy ourselves that information has not been lost or shared with anyone inappropriately, it is important to maintain an “end to end” approach to Information Assurance. There should be a record kept of destroyed files.

For destruction of protected information on electronic medium e.g. Computer containing hard disk, USB memory sticks, optical discs, tape, use only HMPPS approved contractors. Approved contractors can be sourced from the catalogue.

The mandatory requirements and guidance on the appropriate methods of destruction for information classified under the GSC scheme can be found in the Government Security Classification Policy.

The mandatory requirements for how long to retain information for and the appropriate methods of the destruction of paper records are contained in PSI 04/2018 PI 02/2018 AI 03/2018 Records, Information Management and Retention Policy

Specific requirements for the destruction of IT equipment and electronic storage media (e.g. CD’s, DVD’s, and Memory Sticks) is contained in PSI 25/2014 PI 19/2014 AI 19/2014 IT Security Policy.

4.6 Information Loss / Compromise Incidents

Where legislation and regulation requires us to appropriately handle and protect information, those same demands also requires us to report, manage, and in some cases escalate, all events where information requiring protections is either lost or compromised.

Lost is defined as information that either we do not know its location (this can be both internally and externally) or where we suspect its location and it is out of our control. An example of this is a loss through post, where the package is likely with the mail carrier but we have no control over locating it.

Compromise is defined as information that has been subject to unauthorised access, use, or modification. A loss or compromise of information could take many forms and could be discovered in different ways. The list below is not exhaustive, but examples include:

- loss of an offender file, or one found where it should not be,
- information missing in the post or after a fax transmission,
- Information emailed to the incorrect address,
- loss of a computer, laptop, tablet or memory stick,
- loss of a mobile phone or Blackberry,
- leaving a computer disc or laptop or paper document on a train or in any non-secure environment.

Annex A

Transmitting and transporting information assets

1. When considering electronically transmitting information assets:

   - The best option is to hold and access on HMPPS systems within HMPPS premises, including TTP, Quantum or other accredited/assured systems.
   - The second-best option is remote access from an approved remote-access computer on which the information will not be permanently stored.
   - If none of these are possible, the Information Asset Owner may themselves, or authorise others, to use removable media to transfer information.
   - Only a HMPPS approved removable device is allowed (e.g. an approved encrypted memory stick). Information with regards to approved devices and purchasing can be found on the HMPPS Information Security (InfoSec) & Services team support pages on the HMPPS intranet.
   - Only the minimum information necessary for the business purpose should be transferred.
   - Sensitive documents (for example, MAPPA Minutes) should be password protected before sending. The password should be sent in a separate email. Sensitive documents should not be sent to shared or functional mailboxes or attached to calendar invites.

2. When transmitting physical information, you should consider the following, where relevant:

   - Audit-trail / signing out.
   - use of approved couriers (such as DX, Royal Mail Special Delivery).
   - always use return addresses.
   - double envelopes.
   - tracking systems.
   - confirmation of receipt.
   - reporting of undue delays or concerns as potential incidents.

3. Additional guidance on transmitting information can be found in PSI 12/2014 PI 04/2014 AI 10/2014 - Government Secure Classification (GSC) policy.

Transmission by Telephone (Voice) and Skype

4. The public telephone network is not secure. There are a number of ways in which conversations may be intercepted or overheard; mobile phones are particularly vulnerable. Care should be taken not to disclose sensitive information using a normal telephone, this is also applicable when using Skype for business. Skype is not a secure messaging mechanism and care should be used when discussing business matters.

5. Information requiring protection can, if there are no alternative communication routes, be passed over the telephone. The language should be guarded and only the minimum information needed to relay the communication's meaning should be used.

Transmission by Fax

6. Commercial facsimile machines that transmit and receive information over telephone lines are not secure and should only be regularly used for the transmission of information that does not require protection.

Transmission by Postal Services

7. Wherever possible, transmission by trusted hand is the best option. For example, it introduces unnecessary risk to send a transferring Prisoner / Offender's record by post if the record could have been taken by the escort. A risk assessment on the transmission mechanism should always be undertaken before transmitting a new form of information.

8. Information not requiring particular protective measures may be sent by ordinary letter post under single cover (envelope, pouch, etc.). The cover should bear no indication of the classification or sensitivity of the contents.

9. Upon receipt of protected information, if it is suspected that there has been any tampering with the seals or wrappings, an incident investigation should take place and it should be reported in line with the section below on Incidents.

10. If sending Offender correspondence to an address where the addressee will receive it directly, the Information Asset Owner may deem that a single envelope through standard delivery services will suffice.

11. Below is a list of suitable post carriers. It is not an exhaustive list but does identify some recognised providers.

DX

12. DX provides various postal services and document storage / retrieval services to HMPPS and the wider MoJ under an agreed contract. This is a suitable option for sending individual case files, as long as appropriate enveloping is used.

Annex B

The process for reporting a data loss / compromise of HMPPS data

Every staff member, irrespective of role, grade, or location, is required to report an event involving loss or compromise of data.

Incident reporting process

1. Staff that identify a data loss, become aware of or suspect a data loss, must immediately (within one hour) notify the HMPPS Information Security (InfoSec) & Services team via the reporting line number (0203 334 0324) and bring it to the attention of the designated responsible manager, or in their absence, another Manager. The HMPPS Information Security (InfoSec) & Services Team will request that a Security Incident Report form is completed, which can be e-mailed if needed or a template can be found on the HMPPS Information Security (InfoSec) & Services Team page of the HMPPS intranet. It is mandated that the incident must be reported via this Security Incident form and not another version of the form, as this is linked to the teams Incident database.

   While some assessment of the significance of the loss will be apparent in making the initial report, it is important that all losses or potential losses are reported immediately, without waiting for the results of investigations or risk assessments. If in doubt, make contact with the HMPPS Information Security (InfoSec) & Services Team.

   If an incident needs to be reported to the ICO (Information Commissioners Office) then under the new UK GDPR guidelines we only have 72 hours in which to do so.

2. On identifying a possible incident, the lead manager must establish whether it is a potential significant incident. Some of the factors to consider include:

   - the nature of the information (is it personal information or sensitive corporate information?)
   - the number of individual records involved (if personal information)
   - the possible impact of the incident, including the apparent risk to the individuals, their families (for instance, children), staff, victims, offenders under supervision, members of the public and HMPPS / Ministry of Justice's operations or reputation
   - the necessary actions to be taken to mitigate the risk, both immediately and for the future.

3. If the incident is considered serious or impacting, the lead manager must immediately inform the appropriate Senior Civil Servant (SCS), (Deputy Director of Custody, Deputy Director of Probation, Wales Deputy Director Probation and Partnerships, HQ Director) through the management line.

   All contracted providers should report the incident through the contractual line (designated contract manager)

4. Where the incident is escalated to a Senior Civil Servant, it is the responsibility of the SCS to inform the right people within the organisation, to initiate an investigation into the circumstances surrounding the incident and to ensure that it is handled correctly and closed down swiftly, with lessons learnt and next steps documented and followed through.

5. All Senior Civil Servants must ensure that all staff are aware of and have access to this instruction and know what to do in the event of an incident. This includes contractors, temporary staff and third parties who handle personal information.

6. HMPPS Information Security (InfoSec) & Services Team., in discussion with the lead manager and / or Senior Civil Servant must inform the following of significant incidents:

- the News Desk in the Ministry of Justice Press Office
- The HMPPS Senior Information Risk Owner (SIRO)
- The relevant regional office for either Public Sector Prisons or the Probation Service (if not already involved)

7. Some notifications about incidents will inevitably be false alarms. The first stage will be to ascertain whether an incident has in fact taken place or whether it might be a false alarm.

8. The HMPPS Information Security (InfoSec) & Services Team will liaise with the Lead Manager throughout the course of the incident until resolution and closure. If an investigation into the incident is required this will need to be completed within a 28 day period.

Major data Incident procedure

9. If the severity of an incident meets defined criteria, the HMPPS Information Security (InfoSec) & Services Team will alert the HMPPS SIRO for invoking the Major Data Incident procedure.

Incident local investigation

10. Upon confirmation that a loss or compromise has occurred, the Information Asset Owner, or delegated authority to the Information Asset Custodian, must commission a local investigation.

The investigation will inform a risk assessment which should cover the following points:

- numbers and status (e.g. victims) of individuals affected
- type of data compromised (e.g. personal data, sensitive, corporate data, non-sensitive data)
- circumstances of the incident (including physical environment, time of day)
- whether the incident concerns or affects non-HMPPS organisations
- full assessment of the possible risks arising, covering risks to data subjects, the public, Ministry of Justice or government operations and reputation
- the risk of additional loss from a vulnerability being further exploited

11. You are advised to keep notes, especially if the incident is complex or developments are moving fast and details need to be captured.

12. Taken together, these assessments should inform recommendations for next steps and press handling, regardless of whether or not the incident is likely to become public knowledge.

13. Next steps must include recommendations on**:**

- whether and how to inform data subjects (those whose data has been lost / compromised) or other parties. These should be based on an objective and accurate assessment of the statutory duties, the potential risks and the benefits of disclosure
- Informing the Information Commissioner's Office. The HMPPS Information Security (InfoSec) & Services Team, in liaison with the Ministry of Justice Information Directorate, will advise on whether the Information Commissioner's Office should be informed. The

Commissioner can often provide practical advice on handling incidents and where the incident (or potential incident) is very serious we have a duty to inform the Commissioner

- whether the police need to be involved, e.g. if the incident involves MAPPA case information or where the loss involves possible theft of data from premises or systems.

14. The following list is possible questions to ask within the course of a local investigation (note that the list is not exhaustive:

a) Please outline the full facts leading to this incident occurring.
b) What steps did HMPPS take in the immediate aftermath of the incident to prevent further damage to or loss of data?
c) As a result of this incident, did HMPPS consider whether any other sensitive personal data held may be exposed to similar vulnerabilities? If so, what steps were taken to address this?
d) What further action has been taken to minimise the possibility of a repeat of such an incident?
e) It would be helpful if you could provide us with a copy of any internal security breach report produced in connection with this incident.
f) What training does HMPPS provide to its staff in relation to the requirements of the DPA? Does HMPPS intend to review this provision in light of the incident?
g) Had the employee(s) concerned in this received DPA training? If so to what extent?
h) As the data controller, does HMPPS have a security policy which sets out how data of this type should be handled? If so, did the circumstances of this particular incident breach this policy? Please provide a copy of any relevant policy or procedure, or extracts from it specifically dealing with fax transmissions.
i) Do you consider the employee(s) involved has breached the organisation's policy or procedures?
j) Please inform us of any disciplinary action taken, if any, in relation to the employee(s) involved.
k) Is there any evidence to date that the personal data involved in this incident has been inappropriately accessed / processed any further? If so, please provide details
l) Has the data subject been informed about this incident?
m) Has any efforts were made to ensure data recovery post notification of incident?
n) Has any written confirmation on destruction of data has been requested or received? Has HMPPS received a formal complaint from any individual affected by this breach? If so, please provide details.
o) Has there been any media coverage of the incident? If so, please provide details.

HM Prison & Probation Service

Peer Support Non-Disclosure Agreement

All Peer Workers should read this statement before signing their agreement for information to be shared with them under the conditions outlined below. If the Peer Worker has difficulty with reading or understanding the information a member of staff should read through the document before it is signed.

Confidentiality Statement
The personal information you will be given by other prisoners and staff in your role as Peer Supporter at HMP …… must be treated as confidential at all times and must not be disclosed, except to prison staff in your role as a Peer Support Worker.

Your role is to gather and record information for the prison and the prison staff that support the peer worker process. However, if you have been made aware of any safety concerns whilst in the role of a Peer Support Worker, you must report them to any member of prison staff under the following circumstances:

1) **When you have reason to believe that there is real risk of serious harm to yourself or others.**
2) **If you become aware of any offence under the Misuse of Drugs Act 1971 and the Drug Trafficking Offences Act 1986 in respect to the supplying or cultivating of controlled drugs in the establishment.**
3) **If you become aware of any offences under the Child Protection Act 1989.**
4) **If you become aware of any other crime.**

Should you breach this agreement, sharing personal information about other prisoners to a third party who is not entitled to have access to that information, you will be in breach of your compact and Job Description, as well as the Data Protection Act 2018, and may:

- lose your job as a peer support worker
- be adjudicated for breach of Rule 51(23), 'disobeys or fails to comply with any rule or regulation applying to you'
- Receive an IEP review

I agree to abide by the conditions of this agreement and understand the consequences of failing to do so.

Signed by: **……..…..**

Signature: _____

Annex D – Paragraph to be included in all induction packs

Information Sharing for Prisoner Induction Pack

As a new reception prisoner to HMP …….. you will have been provided with a copy of the HMPPS Prisoner Privacy Notice. This advises you of;

- The purpose of collecting your personal information.
- The types of information we collect.
- Why we collect your information and what lawful basis do we have for the collection.
- Who the information may be shared with.
- When we ask you for personal data.
- How to access your personal information.

Specifically trained prisoners Peer Mentors are among those that we may share your personal data with in order to assist you whilst residing at HMP …….., and in order to aid you in a planning your release back into the community.

If you do not wish for us to share your personal information in this way you have a right to object, and if you do object, we will not share your personal information with Peer Mentors. You should make staff aware of your objection at the earliest opportunity, ensuring that your application is placed in a sealed envelope and marked for “Confidential - Staff only to process”.

If you wish to withdraw your consent to share your personal information in this way, you may do so at any time. Again, you should make staff aware at the earliest opportunity, ensuring that your application is placed in a sealed envelope and marked for “Confidential - Staff only to process”.

Annex E – To be included in all Job Descriptions

HM Prison & Probation Service

HMP …….

Job Title: Peer Support Worker

Hours of Work:	
Areas of Access:	
Role Profile:	
Standards and Performance:	• Maintain the confidentiality of the service. • Adhere to you role responsibility compact • • • • •
Comply with:	• Data Protection Act (DPA) 2018 • • • • •
Requirements:	• To attend any additional training or educational classes as required for your role. • To maintain any information or data provided in a secure location. • • •
Correct Clothing:	
Qualifications: (delete as appropriate)	Must be actively working towards/ or hold: • NVQ Peer Mentoring Level 1 • NVQ Peer Mentoring Level 2 • NVQ Peer Mentoring Level 3 • NVQ Peer Mentoring Level 4 • the NCFE Level 2 Mentoring Skills Award • Open Awards Level 2 Certificate in Delivering Information, Advice and guidance. • Other

Failure to comply with any of the above, will result in your immediate removal from the position

I agree to abide by the terms of my job description and will undertake my duties within my area of responsibility in accordance to the relevant schedules and safer systems of work

Name (print) …….. Date……

Signature ……

Officer/ Member of Staff (print)…… Date ……..

Signature……