Legal Aid Agency

Data Security Guidance

LAA Information Security – Sept 2024

This document shall be amended in accordance with the relevant LAA Contract by releasing a new edition of the document in its entirety.

Version Control

Version	Issue date	Last review date	Owned by
4	01/09/2024	September 2024	LAA Corporate Assurance Team

Version History

Paragraph	Changed From	Changed To	Comments
All (Sept 2024)		Current LAA format	Format has been updated
All	Legal Services Commission (LSC)	Legal Aid Agency (LAA)	All references to LSC have been updated to LAA
All (Nov 2020)	Regulation (EU) 2016/679	UK GDPR	All references to GDPR have been updated to refer to UK GDPR.
All (Nov 2020)	GDPR	UK GDPR	All references to GDPR have been updated to refer to UK GDPR.
All	Data Protection Act 1998	Data Protection 2018	All references have been updated to reflect the new legislation and any references to specific sections of the 1998 Act removed.
All	References to the Government Protective Marking Scheme (GPMS)	References, where necessary, to Government Security Classification system (GSCS).	GSCS replaced GPMS in 2014. GSCS only requires personal data to be marked by exception where higher/specific markings are required.

All (Sept 2024)			Requirements renumbered – all references to Requirements have been updated to reflect new numbering introduced in Version 4. Paragraphs have also been reordered and renumbered to match the Requirements order.
Table of reference documents			All links/documents have been updated to quote the latest versions.
Table of reference documents (Sept 2024)	HM Government Security Policy Framework	Government Functional Standard GovS 007 - Security	
2.1		[INSERTION] Also relevant to barristers are the 'Guidelines on Information Security' on the Bar Councils website: https://www.barcouncilethics.co.uk/documents/information-security-3/	Updated to include latest version of Bar Council's guidance.
2.3 (Nov 2020)			Definition of sensitive data updated to reflect wording in legislation and ICO guidance.
2.4 (Sept 2024)			Definition of Information Asset has been updated to provide clarity and moved from Part 3 to 2.4
2.5 (Sept 2024)	[REMOVED] Paragraph on Data Handling Cycle	[INSERTION] Complete paragraph on information life cycle	The section on data handling cycle no longer aligned with current practice.
2.6	[REMOVED] The Legal Services Commission (LSC) [INSERTION] All contracts include specific requirements Reference to the Access to Justice Act (1999) has been removed as has a statutory obligation to establish, maintain and develop the Legal Aid Scheme i.e. the Community Legal Service ("CLS") and the Criminal Defence Service ("CDS") under the Access to Justice Act (1999).	[INSERTION] All contracts include specific requirements for preserving the security of the information Providers receive from LAA and also share with the LAA.	Reference to the Access to Justice Act 1999 has been removed as this is no longer relevant.
3	Roles and responsibilities diagram removed		

3.2 (Sept 2024)	[REMOVED] All Providers should	[INSERTION] All Providers must	Introduction to bullet point list changed from “should” to “must” to reflect that Requirement 4 is a mandatory requirement.
3.2 (Sept 2024)	Ensure training sessions highlight key policies and procedures and give individuals the chance to ask questions and receive clear advice related to their function	Ensure training sessions highlight key policies and procedures (including LAA specific policies that Providers must adhere too) and give individuals the chance to ask questions and receive clear advice related to their function	Added additional emphasis to ensure there is clarity that key policies include those published by the LAA for Providers.
3.3 (Sept 2024)	**Data Handling Policy Document** To ensure good data handling practices, all Providers should have a Data Handling Policy in place, which as a minimum meets the following requirements:	**Data Handling Polices** To ensure good data handling practices, Providers must have policies that cover data protection compliance, the management of information risk, IT security, data classification and the security standards/expectations for staff working remotely / at home. We recommend policies that detail Clear Desk processes, information security practices, including the use of removable media and reflecting performance against information and security policies within a Provider’s HR standards. These policies should create one or more documents that detail data handling practices for both physical and electronic data across the organisation.	The guidance on a data handling policy document no longer aligned with the referenced requirements to hold multiple documents dealing with different aspects of data handling.
3.3 (Sept 2024)		[INSERTION] Where a Provider security incident involves Shared Data and meets the threshold for reporting to the Information Commissioner’s Office (ICO) the Provider is responsible for reporting. The Provider should inform the LAA, via their Contract Manager, of the report and of any actions or recommendations made by the ICO.	Clarify responsibility for reporting to ICO where an incident arises with a Provider and Shared Data.
3.4 (Sept 2024)		[INSERTION] All text for this section is added for this version.	Existing text on LAA auditing moved to 4.1
3.5 (Sept 2024)		[INSERTION] Providers should have a mechanism in place to ensure that staff members can raise concerns and that staff members that do so will not be treated unfairly.	No guidance was previously provided on Requirement 9.
3.5 (Sept 2024)	Checks with the Criminal Records Bureau.	Checks with the Disclosure and Barring Service for criminal records.	Updated CRB checks to DBS checks, reflecting current UK process.

3.5 (Sept 2024)		[INSERTION] Access to LAA Systems In order that the LAA can maintain effective access controls across LAA online systems, user accounts for the LAA Online Portal are for individual use only. Accounts shall not be created for offices. Sharing of passwords between individuals, or shared use of an account is prohibited unless explicitly authorised by the LAA. Such authorisation may be sought from your Contract Manager in exceptional circumstances.	Additional guidance on password sharing for LAA systems only.
3.5 (Sept 2024)		[INSERTION] Added new paragraphs to expand on physical security guidance.	
3.10 (Sept 2024)		[INSERTION] Further Guidance is available separately for Provider's submitting removable media to the LAA. This can be found on gov.uk	Linked this guidance to the separate removable media guidance
3.12 (Sept 2024)		[INSERTION] Added paragraphs on Secure File Exchange and third party file sharing sites.	
3.12 (Sept 2024)		No data may be transferred outside of the EEA without prior written authorisation from the LAA	Line added to clear inconsistency and for clarification
3.13 (Sept 2024)		[INSERTION] New paragraph added to provide guidance on new requirement 28	New paragraph on multi-factor authentication.
4.2 (Sept 2024)		Remote access should be to a secure network owned by the provider. Data must not be stored in cloud storage unless that cloud storage is hosted within the EEA.	Added for clarity and to ensure data is not sent outside the EEA
4.4 (Sept 2024)		[INSERTION] Risk assessments should also be backed up with hands on security testing on systems which store, process or transmit records on large numbers of individuals.	

Contents

Referenced Documents

The following is a list of documents with a direct bearing on the contents of this guidance.

Ref.	Title	Date / Version	Author
1	Data Security Requirements	v.4 September 2024	Legal Aid Agency
2	Data Protection Act	2018	HMSO
3	Government Functional Standard GovS 007 – Security	July 2020	Cabinet Office
4	ISO 27001	2013	International Standards Organisation
5	ISO 27002	2013	International Standards Organisation
6	LAA Privacy Notice	May 2022	Legal Aid Agency
7	LAA Information Charter	v.4 August 2021	Legal Aid Agency
8	Handling Removable Media	January 2020	Legal Aid Agency

1. Scope

The nature of the services provided by the Legal Aid Agency (LAA) means that clients will entrust the LAA with their personal data, some of which may be sensitive in nature. The LAA has an Information Charter which provides assurance to clients that it will keep their data secure at all times.

LAA requires Providers[1], and any third parties appointed by Providers in accordance with the LAA contract, to have secure organisational and technical measures in place to protect such personal data from unlawful or unauthorised processing, accidental loss, destruction or damage and to maintain the confidentiality, integrity and availability of information.

The Data Security Requirements (DSR) sets out the mandatory and recommended requirements which must and should be adhered to as required by the contracts between LAA and the Providers. The intention of this Guidance is to make Providers involved in the administration of Legal Aid aware of the policies, principles and requirements that govern the obtaining, use, storage and destruction of “Personal Data” (defined below).

This Guidance explains what the Providers (including their employees and any further third parties they appoint in accordance with the contract) responsibilities are under the Data Protection Act 2018 (DPA), UK General Data Protection Regulations (UK GDPR) and the Government Functional Standard GOV007 Security (GFSS).

Providers should also ensure that any third parties appointed by Providers in accordance with the LAA contract are also following this guidance. This can, in part, be achieved by providing copies of this document and the DSR to any third parties appointed by Providers.

If we authorise you to perform Remainder Work, the terms of the contract, including the DSR will continue in force and effect for that Remainder Work.

2. Scene Setting

2.1. Overview

Information is a key asset to Government and its correct handling is vital to the safe and effective delivery of public services. Departments and agencies of the government need to be confident that their information assets are safely and securely stored, processed, transmitted and destroyed, whether managed by the organisation or by delivery partners and suppliers. Equally, Government has a legal obligation and duty to safeguard personal data entrusted to it by citizens and businesses. In striking the right balance between enabling public services and sharing and protecting data, organisations must assess and

[1] A Provider means a party other than the LAA to a contract with LAA in respect of the provision of legal services funded by LAA.

manage the risk to the services they provide and to confidentiality, integrity and availability of the information assets they are formally responsible for.

All Government Departments and Providers process and manage increasing amounts of Personal and Sensitive Data, collectively referred to in this document as “Personal Data”, therefore it is imperative that clear guidance is available which defines Department’s and Providers responsibilities towards that data. This document is based around the GFSS and its supporting documentation, the data protection requirements and security good practices set out in ISO 27001 and ISO 27002.

For solicitor’s practices the Law Society publishes a variety of guidance, practice notes and tool kits on data protection and information security.

For barristers’ the Bar Council publishes a guide on information security good practice available on the ethics hub

https://www.barcouncilethics.co.uk/wp-content/uploads/2019/11/Information-Security-Jan-2021-1.pdf

2.2 Definition – Personal Data

The DPA defines “Personal Data” as “any information relating to an identified or identifiable living individual”, also known as the Data Subject. Whilst the DPA refers to living individuals, the principles in this guidance also apply to deceased individuals and their records.

In addition, the data subject must be the focus of the information concerned. The information has to be able to convey something of significance about that individual and includes any expression of opinion about the individual and any indications of the intentions of the data controller or any other person in respect of the individual.

The following list provides non-exhaustive examples, relevant to the work of the LAA, of the types of personal data which may be held:

- Parties involved in a case
- The party’s names and addresses
- The merits of a case
- Details of a case
- Information required to judge the merits of a case
- A case reference number
- Financial eligibility details and contribution amounts made by parties
- Fee schemes that apply to a case
- Bills and payments
- Customer service information
- Dates of birth
- National Insurance Numbers (NINOs)
- Details of criminal charges.

LAA and Providers need to abide by the 7 Data Protection Principles of the UK GDPR when handling Personal Data. These can be found in Annex 1

2.3 Definition – Sensitive Data

There is no single definition of sensitive data. UK GDPR defines special category data and data relating to criminal offences as data requiring additional protections because of their sensitivity. DPA details a similar list of sensitive data in the context of processing for law enforcement purposes.

Special category data is personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life, and data concerning a person's sexual orientation. Any data that reveals or concerns the above categories will be treated as special category data.

The LAA may specifically collect, or require Providers to collect, some of these categories. Providers should be aware that even where not specifically collected, the details of a case or details required to judge the merits of the case may, by the nature and circumstances of the case, reveal or concern special category data about a data subject, whether a client, opponent or other party to proceedings.

Criminal offence data covers a range of information relating to criminal activity, allegations, investigations, proceedings and may include information on unproven allegations, information relating to the absence of convictions, personal data about penalties or other conditions or restrictions imposed as part of a criminal justice process and the personal data of victims and witnesses.

The LAA and Providers are required to process criminal offence data for all forms of criminal legal aid. Providers should be aware that criminal offence data may arise in civil proceedings as well, for example in the details of a case, or in details required to judge the merits of a case.

Separately to data protection legislation, the Government Security Classification system (GSCS) provides additional protections for OFFICIAL material which has particular sensitivity, marked as OFFICIAL-SENSITIVE. Providers are required to adhere to and apply the GSCS under Requirement 05a.

Cases that might be considered as particularly sensitive under GSCS are those where there is a specific risk assessment or threat to a highly vulnerable individual, cases involving intimidation, corruption or large scale fraud, cases where there is a legal requirement for anonymity, cases where there is a high media profile and risk of damaging consequences if information is not handled securely, serious and organised crime cases, cases where there is a risk of harm to children, cases involving forced marriage protection orders, and cases where the client is living in a refuge. This list is not exhaustive.

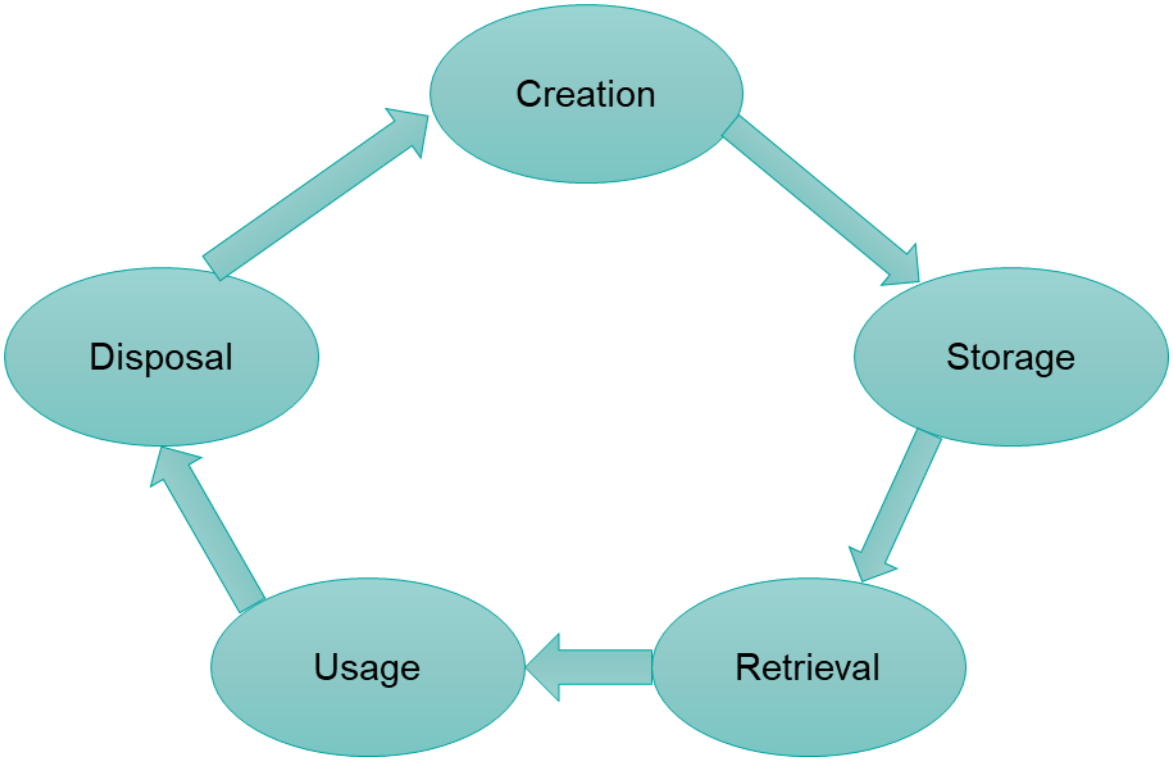
Annex 3 sets out more information about the GSCS and the types of data that fall under the different classifications.

2.4 Definition - Information Assets

An information asset is a single item or set or body of information, managed as a single unit, so it can be understood, shared, protected and exploited effectively. It can be a single significant record or document, or a set of related data, documents or files. It can be shared or be confined to a specific purpose or organisational unit. Information assets have recognisable and manageable value, risk content and lifecycles. Many information assets will be key IT based systems, electronically held documents, spreadsheets etc. Some information assets may only be held in hard copy. This Guidance applies equally to information assets held in electronic or physical form.

2.5 Information Life Cycle

All information and therefore all Information Assets have a life cycle. Security must be considered at each stage of the life cycle and Providers must ensure their policies and procedures consider each of the stages. The Requirements and information in this guidance will assist Providers in protecting information assets at each of the stages.



2.6 LAA Contracts

All contracts include specific requirements for preserving the security of the information providers receive from the LAA and also share with the LAA.

The DSR sets out the minimum requirements to which Providers must adhere and recommendations for other principles that Providers should consider. This document provides the guidance on how those requirements should be met. It includes references to the DSR and then sets out more information about the types of actions that Providers are expected to carry out in order to meet those requirements.

3. Guidance for Requirements

3.1 Governance

The DSR requires that providers must adhere to the following requirements.

Requirement 01	Register as a Data Controller	Mandatory	To be registered as a Data Controller with the Information Commissioner's Office unless an exemption applies.
Requirement 02	Appoint a Data Protection Supervisor	Mandatory	Appoint a senior member of staff as a Data Protection Supervisor with overall responsibility for data protection and information security.

The term "Data Controller" is defined within the DPA to mean 'a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.'

The Data Protection Supervisor is used in these documents to refer to the specific individual with responsibility for data protection and information security within the Providers' organisation.

To ensure that data handling is properly embedded within the organisation's culture, there must be strong accountability from the Provider senior management team. By nominating key individuals to manage, monitor and help resolve issues, organisations can ensure that issues are standardised and will enhance the processes by which organisations understand and manage their information risk.

3.2 Culture

The DSR requires and recommends that Providers adhere to the following requirements.

Requirement 03	Foster a culture that values and protects information	Recommended	Have plans in place for fostering a culture within the organisation that values, protects and uses information for the public good and in accordance with the Principles relating to processing personal data as defined in UK GDPR.
Requirement 04	Maintain a level of staff awareness	Mandatory	An induction plan to raise awareness to new staff on data protection obligations and information risk awareness and an annual training plan, as appropriate, to maintain the level

			of staff awareness of obligations with policies and procedures.

It is critical that good practices in both security and data protection are embedded within the business culture of all Providers. These standards should be set by the senior management and transferred through the entire team of the Provider.

It is essential that the right example is set at the top. High levels of data security must be underpinned by a culture that values, protects and uses information. This culture is important both when services are being planned and when they are being delivered.

The senior management of a Provider should document a plan or policy setting out how they will foster, develop and maintain such a culture.

It is then important that adequate guidance and training is given to all employees, especially those handling personal data. Training should motivate change within personnel to improve and ensure information security and awareness.

All Providers must:

- Provide training courses which are deemed essential for staff roles identified within their organisation;
- Provide training to all staff on handling Personal Data;
- Be assured they have a consistent approach to training;
- Cover obligations relating to Data Protection, IT security, records management and privacy education
- Ensure training sessions highlight key policies and procedures (including LAA specific policies that Providers must adhere too) and give individuals the chance to ask questions and receive clear advice related to their function;
- Ensure training is regularly refreshed and not just a one off;
- Maintain content and version control for information security and privacy training materials and make these available for audit inspection if required.

3.3 Policies

The DSR requires and recommends that Providers adhere to the following requirements.

Requirement 05a	Have a coherent set of policies	Mandatory	Must have policies covering: • Information Risk Management • Data Protection compliance • IT Security, including an acceptable use policy • Compliance with the Government Security Classification System • Remote/Home Working Policy detailing security arrangements/procedures (where

			such working is permitted by the Contract).
Requirement 05b	Have a coherent set of policies	Recommended	Should have policies covering: • Clear Desk Policy • Information Security, to include restricting use of removable media • HR standards that reflect performance in managing information risk and complying with above policies, incorporating sanctions against failure to comply.
Requirement 06	Undertake an annual review	Recommended	To have in place procedures to review all data protection and information security policies at least annually.
Requirement 07	Have in place an incident management policy	Mandatory	Have a policy for reporting, managing and recovering from information security incidents, including losses of personal data, IT security incidents. Policy must define responsibilities, including responsibilities to notify the LAA of relevant incidents. Staff must be made aware of the policy.

To ensure good data handling practices, Providers must have policies that cover data protection compliance, the management of information risk, IT security, data classification and the security standards/expectations for staff working remotely / at home. Providers must also have a policy for responding to, managing and recovering from an information security incident, including personal data incidents.

LAA requires that Providers implement the Government Security Classification system, and that material is marked appropriately in accordance with this system. Details on the GSCS are set out in Annex 3.

We recommend policies that detail Clear Desk processes, information security practices, including the use of removable media and reflecting performance against information and security policies within a Provider's HR standards.

These policies should create one or more documents that detail data handling practices for both physical and electronic data across the organisation.

These practices should be:

- Clearly documented
- Reviewed and updated regularly, and at least annually
- Distributed to all staff at least in summary form, with full details provided to all relevant staff
- Easily accessible to all staff and specifically drawn to the attention of new staff; and

- Conform to ISO 27001 and ISO 27002 good security practices. Providers are not required to be certified to this standard, however they must provide written confirmation that any information assets as identified in section 2.4 are managed in line with best practice as detailed in this standard.

Specific technical requirements that may form part of the content of these policies can be found in subsequent sections of this Guidance.

All Providers must have a documented Incident Management process in place which incorporates the following:

- A procedure for reporting, managing and recovering from information security incidents, including the loss of personal data and incidents involving IT system failures or compromises.
- Set out that the Provider must inform the LAA, via their Contract Manager, within **1 working day** of becoming aware of a loss of data or suspected security incident of any kind and then follow any instructions received from the LAA. This includes incidents where a provider's system has become infected or exposed to malware, virus or malicious code.
- A statement setting out that Provider staff will provide details of the exact nature of any data security incident to the LAA.
- Confirmation that the Provider will take all responsible action to prevent the future loss of data.

The LAA has defined internal processes and guidance in place for responding to incidents raised by Providers.

Where a Provider security incident involves Shared Data and meets the threshold for reporting to the Information Commissioner's Office (ICO) the Provider is responsible for reporting, and where necessary, informing the data subject. The Provider should inform the LAA, via their Contract Manager, of the report and of any actions or recommendations made by the ICO.

3.4 Compliance

The DSR recommends that Providers adhere to the following requirement.

Requirement 08	Monitor and Report	Recommended	Monitor compliance with data protection and security policies and produce an annual audit report.

Providers should regularly review and/or assess the implementation of the DSR within their organisation. Providers should produce an annual reporting documenting their compliance that may assist the Provider in demonstrating compliance to the LAA on audit. Such reviews/assessments will help to identify weaknesses that can in turn be rectified, improving the security of Personal Data processed by the Provider. A checklist compliance tool is included with this Guidance at Annex 4.

3.5 Procedures

The DSR requires and recommends that Providers adhere to the following requirements.

Requirement 09	Implement a 'whistle-blowing' procedure	Recommended	Implement mechanisms for raising concerns about information security or any incidents or breaches of the DPA or related policies.
Requirement 10	Conduct Data Protection Impact Assessments	Mandatory	Where appropriate, conduct data protection impact assessments of any new system or projects, in compliance with Information Commissioner's Office guidance.

It is important that all Providers can demonstrate strong governance to provide the assurance necessary that data is being handled responsibly and to minimise the risk of any security incidents. Providers should have a mechanism in place to ensure that staff members can raise concerns and that staff members that do so will not be treated unfairly.

All Providers must conduct Data Protection Impact Assessments in compliance with guidance issued by the ICO.

Requirement 11	Conduct staff screening	Mandatory	Conduct appropriate screening of staff and carry out background checks to ensure reliability.

It is essential that the LAA can be confident that the individuals employed by Providers are who they say they are.

Security is of great importance to the LAA. A key element of achieving a level of security is determining a level of 'trust' in the individuals working for an organisation. Therefore, all Providers must consider their vetting process for new recruits, agency staff and current employees, especially those with the highest privileged access to large volumes of claims data. As an example, the vetting process might typically include:

- Previous employment references;
- Verification of home address;
- Checks for County Court Judgements, Insolvency Voluntary Arrangements and Bankruptcy;
- Checks for Directorships on Companies House and where relevant, checks on disqualification from being a Director;
- Checks with the Disclosure and Barring Service for criminal records.

Requirement 12	Control access to personal data	Recommended	Introduce a mechanism for controlling access to personal data and restrict access to authorised staff only and

			restrict access to the minimum personal data necessary / relevant to the job role.
Requirement 13	Maintain access records	Mandatory	Maintain records of staff, agents and approved third parties' access to personal data and an audit trail of activities undertaken on it and review audit trail for compliance with policies.

Access controls are essential to keep data secure and ensure that it is only accessible by authorised individuals.

Providers must conduct regular reviews of staff access rights to ensure:

- That all users who have access to a system are authorised to handle the data;
- That individuals have the correct access privileges in accordance with their job roles, and that users do not have excessive access rights to a system.
- That all staff that have left the organisation or no longer need access to a system, premises or location are identified and access removed as soon as possible.
- That physical locations protected by combination locks or door codes have the codes changed when staff leave to remove access.
- That system users with administration, "super-user" or other privileged access rights are checked to see if they have a justifiable reason for having these privileges.

Providers must maintain records of staff, including third party staff with access to Personal Data, whether stored in physical files or electronically. Providers must maintain audit trails of access and activities undertaken on Personal Data and review audit records to monitor compliance with policies.

Access to LAA Systems
In order that the LAA can maintain effective access controls across LAA online systems, user accounts for the LAA Online Portal are for individual use only. Accounts shall not be created for offices. Sharing of passwords between individuals, or shared use of an account is prohibited unless explicitly authorised by the LAA. Such authorisation may be sought from your Contract Manager in exceptional circumstances.

Requirement 14	Maintain adequate physical security	Mandatory	Introduce and maintain adequate physical security for premises that are used to store, process, or transmit personal or sensitive information. Provide secure areas for storing personal and sensitive information.

Providers must ensure their physical working environment provides appropriate security, for protection of data being processed or stored within the premises. Providers should consider a layered or "defence in depth" approach to ensure that should their premises be

breached, further layers of defence, such as locked storage or secure storerooms are used to protect information assets.

Providers should consider the particular needs of rooms containing server equipment or other similar IT assets.

It is important to ensure that all documents containing personal data are placed in locked cupboards, drawers or secure storeroom when not in use. If files containing personal data are in a hard copy format and contain data classified as OFFICIAL-SENSITIVE they must be clearly marked and kept in a locked cabinet with access limited to only those that require access to the file (see also – Requirement 12).

As well as human threats to premises, Providers should consider environmental threats such as fire, flood, damp or smoke damage and take proportionate approaches to protect information assets in the event of an incident.

3.6 Destruction and Disposal

The DSR requires and recommends that Providers adhere to the following requirements.

Requirement 15	Implement controlled disposal of records	Mandatory	Destroy electronic and manual records containing personal or sensitive information by incineration, pulping, or cross shredding so that reconstruction is unlikely.
Requirement 16a	Secure disposal	Mandatory	Dispose of electronic media holding LAA Data or Shared Data through secure destruction
Requirement 16b	Secure disposal	Recommended	If electronic media is to be reused then it should be securely overwritten or degaussed first. However, reused electronic media is still subject to the mandatory disposal requirements (16a) upon permanent disposal.

The DPA states within the fifth principle that “data shall not be kept for longer than is necessary”. Data should therefore be destroyed when it is no longer necessary to retain it.

When destroying data it is important to ensure that this undertaken in a secure way, to prevent Personal Data believed to have been destroyed being disclosed to or recovered by a third party.

Hard Copy Destruction

There are several ways in which documents should be destroyed.

Shredding can be used to destroy personal data that is no longer required. This should be done using cross-cut shredders with a fine cut of at least 6mm or less. Ribbon shredding is not approved. Incineration may also be used.

Many organisations may use a confidential waste system and contractor. Material placed in confidential waste must be kept secure until collected for destruction. Organisations should obtain and store destruction certificates from their contractor.

Electronic Copy Destruction
As soon as data held in an electronic form reaches the end of its retention period, it should be deleted in a secure way. This means the data must be unrecoverable and cannot be retrieved by simply undoing the last action or restoring the data from a “recycle bin”.

Removable media should have the data wholly overwritten by multiple passes or degaussed. Where the media is not capable of overwrite or degaussing, or where permanent disposal is required it must be completely destroyed via disintegration, pulverisation, incineration or shredding.

3.7 Risk Assessment

The DSR recommends that Providers adhere to the following requirements.

Requirement 17	Conduct formal, documented risk assessments.	Recommended	Conduct formal, documented risk assessments for all systems that store, process or transmit personal or sensitive information when those systems undergo significant changes, or at least every 3 years
Requirement 18	Apply appropriate controls	Recommended	Risk assessments must identify the assets, analyse and evaluate the risks to confidentiality, integrity and availability of those assets and identify and evaluate the options for treatment of those risks. Controls and control objectives for risk treatment should be selected from Annex A to ISO 27001, additional controls and control objectives may also be selected.

It is important that all Providers can demonstrate strong governance to provide the assurance necessary that data is being handled responsibly and to minimise the risk of any data leakage incidents.

All Providers should identify, manage and take actions to mitigate any risks surrounding the production, storage, use, transfer, destruction, deletion or any other processing as defined in UK GDPR in respect of personal data. This includes regular reviews for all processes and procedures, impact assessments of all processes and procedures, including formal Data Protection Impact Assessments where required or recommended and checks to confirm how robust the processes in place are in “business as usual” situations.

Risk assessments should be reviewed whenever there has been a significant change to the system or process, or as a minimum every 3 years.

3.8 Standards and Testing

The DSR recommends that Providers adhere to the following requirements.

Requirement 19	Cyber Essentials Plus	Recommended	To hold Cyber Essentials Plus certification and renew / maintain as required.
Requirement 20	Conduct independent penetration testing	Recommended	Independent penetration testing of systems that store, process or transmit information relating to 100,000 or more identifiable people.

Many areas of Government procurement require suppliers that will be processing personal or sensitive date to hold cyber essentials or cyber essentials plus certification. Some specific LAA contracts may require Cyber Essentials as a mandatory requirement, identified during the tender process. All Providers are recommended to hold cyber essentials plus.

Cyber essentials is a simple but effective Government backed scheme that will help protect your organisation against a range of cyber attacks. More information is available from the National Cyber Security Centre.

LAA recommend that Providers conduct independent penetration testing of their systems to provide additional assurances and identify security weaknesses and vulnerabilities if those systems store, transmit or otherwise process records relating to 100,000 or more identifiable people. Providers may consider this a valuable exercise for systems holding smaller volumes of data too.

3.9 Business Continuity

The DSR requires Providers to adhere to the following requirements.

Requirement 21	Ensure Business Continuity	Mandatory	Create and implement business continuity plans. Create and implement disaster recovery plans.

All Providers are required to maintain both business continuity and disaster recovery plans.

Business continuity (BC) is the ability to maintain a defined level of service during an adverse event or incident. Disaster recovery (DR) is the ability to return to business as usual operations following an adverse event or incident.

Provider's must ensure plans for both BC and DR are in place, in order to maintain service during an incident and recover from the incident. The plans should ensure that the security of information processed by the Provider is maintained.

The plans should be tested at least annually to ensure that they can operate as expected and that DR plans can restore service within an acceptable time frame.

3.10 Security – Storage and Encryption

The DSR requires and recommends that Providers adhere to the following requirements

Requirement 22a	Hard disk encryption	Mandatory	All computers, including laptops, storing personal or sensitive information shall be protected by hard drive disk encryption at a minimum with access controlled by at least username and password as a means of authentication.
Requirement 22b	Hard disk encryption	Recommended	It is recommended that the hard disk encryption product is compliant to FIPS-140 standard.
Requirement 23a	Encryption of removable media	Mandatory	Removable media (defined below) used to store personal or sensitive information shall be protected using encryption.
Requirement 23b	Encryption of removable media	Recommended	It is recommended that the encryption used is AES encryption of at least 128-bit strength.
Requirement 24	Encryption of Personal Electronic Devices	Mandatory	All PEDs (mobile phones, tablets, etc) used to store personal or sensitive information must have device encryption enabled in addition to device access controls.

Laptops and Computers

All types of electronic data storage devices, whether computers and laptops, removable media, or other mobile and personal devices such as smart phones and tablets must use encryption methods to protect the data on the device.

Computers and laptops must use hard disk encryption and also have password requirements for each user account on the device. Ideally, the encryption should be to FIPS-140 standard. Once a laptop will no longer be used, arrangements must be made to wipe data securely from the hard-drive (see also – Requirements 15 & 16). The ability to remotely lock or wipe a laptop in the event of theft/loss is also recommended.

Removable Media

Removable media includes any storage device that can be removed from a computer or other device and is used to store personal data. This can include, but is not limited to, USB

memory sticks and flash drives, CDs, DVDs, SD cards and removable / external hard drives.

All Providers must ensure that the use of removable media for processing Personal Data is kept to a minimum and if possible, not used at all. Where such use is unavoidable, the media must be encrypted, ideally using AES encryption of at least 128-bit strength. Removable media containing personal data must be kept in locked cupboards, drawers or secure storeroom when not in use.

The LAA recognises that Providers may receive case material from third parties on such media and that Providers have limited control over this. Where such material is received Providers should ideally transfer the data to their electronic storage and securely erase or destroy the removable media. If that is not possible, Providers must encrypt the media in accordance with these requirements and store it securely.

Third parties sending personal data to a Provider have their own responsibilities to ensure that the personal data is protected. Where a third party has used alternative methods to secure the personal data that provide sufficient protection to meet the obligations under Data Protection Legislation the Provider should obtain and retain assurances from the third party that appropriate protection is present on the media.

Further Guidance is available separately for Provider's submitting removable media to the LAA. This can be found on gov.uk[2].

Personal Electronic Devices
PEDs include personal digital assistants, smart phones, tablets and any other electronic device capable of storing data and being transported with the user, excluding laptops and removable media detailed above.

PEDs may be used for a variety of functions and may not be used for accessing or storing personal data. Where PEDs are used for storing or accessing personal data appropriate security must be in place and such PEDs should be treated in similar ways to laptops.

In particular, the PED must have device encryption enabled. PEDs that do not offer encryption must not be used for storing or accessing personal data, including through the use of Provider email or other web-based systems.

In addition, any PED used for storing or accessing personal data must:

- Have an active screen locking system in addition to device encryption, using either a passcode, PIN or biometric authentication to unlock.
- Have the ability to lock the device or erase its contents after a predetermined number of failed password attempts;
- Be securely disposed of at the end of the device's lifecycle (see also – requirements 15 & 16)
- Be fully patched/updated

[2] Handling Removable Media

Cloud Storage
Where Provider's use cloud storage solutions Providers must ensure that the appropriate security and segregation of personal data is in place. Personal data must not be stored in cloud storage hosted outside the EEA.

All Providers must ensure that information stored in a cloud system is stored in such a fashion that access is limited to authorised individuals and that any information transferred to a third party and any backups are encrypted.

3.11 Security – Backups

The DSR recommends that Providers adhere to the following requirements

Requirement 25	Regular encrypted backup	Recommended	Backup of all data on a daily basis, as required. Particular care must be taken to ensure the physical security of any unencrypted media.

All systems and services with Personal Data must be backed up regularly. The DSR recommends that daily backups are made and that backup data is encrypted.

All Providers should have a clear written backup procedure and secure mechanisms in place to ensure that the data is secure at all times, both in transit and in storage. All backup arrangements should be tested regularly to ensure that they will operate effectively if required.

Where any data is transferred as part of a backup to a remote secure location, encryption should be used. Arrangements to restore from backups should be tested at least annually. Providers must be able to retrieve information from backups if required. Providers must ensure that when personal data is destroyed from primary systems in line with retention policies, that backup copies of that data are also securely destroyed.

3.12 Security – Data Transfers

The DSR recommends that Providers adhere to the following requirement

Requirement 26	Secure transfer	Recommended	Appropriate protection must be provided to protect the confidentiality, availability and integrity of personal or sensitive information transferred from one physical location to another or transmitted electronically.

Everyone should be made aware of the risks of sending hard copy and electronic data. Before sending any item, Providers should question what information is being sent and whether the method proposed is sufficient, given the nature, sensitivity and classification of

the contents, to enable safe and secure delivery. Providers should also take into account the volume of data sent in a single package.

Sending data by post
All Providers must ensure that all bulk personal data being sent by post must either be sent by Royal Mail Special Delivery, DX Secure or via a contractor that allows for tracking at each stage of the delivery process and captures proof of delivery. Records or data must be in a sealed envelope.

All Providers must ensure that all media devices / data are encrypted, ideally using AES encryption of at least 128-bit strength (see also Requirements 23a and 23b). The content of devices holding personal data should be readily identified without prior knowledge of the content.

Sending data electronically
All data sent by electronic methods should be protected using encryption methods.

Data sent via or uploaded to LAA systems (such as CCMS, eForms) is protected by the use of Secure Sockets Layer (SSL).

In some circumstances, the LAA will exchange data with Providers by email. Ordinary email is not secure and Providers should avoid sending personal data by email where possible. Material classified as OFFICIAL-SENSITIVE must not be sent by ordinary email.

Criminal Justice Secure Email (CJSM) is a secure email system that can be used for sending personal data, including personal data. Use of CJSM is not mandatory, but it is recommended that all providers subscribe to this service.

https://www.cjsm.net

The LAA uses Secure File Exchange (SFE) for the secure submission of bulk electronic data. Use of SFE is not mandatory, but it is recommended that all providers are set up for use.

Providers should be aware that LAA staff will not be able to access, download or view material from third party upload or file sharing sites. Providers using such sites must establish the security afforded to personal data uploaded to the site and in particular ensure that the personal data is hosted exclusively within the EEA unless permission is received from the LAA.

Sending data overseas
Data that is sent overseas must conform to Section 18 of the Data Protection Act and Articles 44-50 of UK GDPR.

No data may be transferred outside of the EEA without first seeking written authorisation from the LAA. No data may be transferred abroad within the EEA without the LAA’s prior authority. When sending data abroad electronically, the level of encryption employed must be at least equivalent to that set out for the UK, unless there is a legal restriction on

encryption in the receiving country. In this case, advice must be obtained from the LAA on a suitable transfer method.

Before sending data overseas Providers should confirm that they have:

- Identified the purposes for making transfers of personal data abroad e.g. legal reasons or data is processed overseas;
- Confirmed whether checks have been made in the receiving country to ensure that similar or greater protection to that afforded in the UK is available;
- Confirmed that they have followed the requirements of Article 44 of UK GDPR and guidance issued by the Information Commissioner's Office (ICO) for overseas transfers;
- Confirmed whether checks have been made to ensure that the transfer of data is acceptable under local privacy laws;
- Standard LAA contractual provisions in place around the transfer of data;
- Obtained written approval from the LAA;
- Considered transparency requirements in respect of the data subjects.

3.13 Security – Malware Protection

The DSR requires that Providers adhere to the following requirement

Requirement 27	Malware protection	Mandatory	Anti-virus and anti-spyware must be installed and kept up to date on all servers, desktops and laptop computers used to store, process or transmit personal or sensitive information.

Anti-malware refers to the detection and prevention of any malicious software from operating on a network, system or device. Malware may include viruses, but also trojan horses, worms and ransomware. Phishing emails are now the most common way for malware to enter a system.

A provider must have in place a policy for ensuring that appropriate anti-malware protection is used to protect their systems and is kept updated. A provider must also have in place documented procedures for staff to follow in the event they identify malware on their device or their device is behaving oddly. These procedures may form part of wider IT security or other policies or procedures.

A provider identifying malware on their system or device must notify the LAA via their Contract Manager at the earliest opportunity so that the LAA can assess the risk to LAA systems.

3.14 Security – Multi-factor Authentication

The DSR recommends that Providers adhere to the following requirement.

Requirement 28	Multi-factor Authentication	Recommended	Multi-factor authentication should be used for all email accounts and any IT system, including cloud systems, storing personal data.

Multi-factor authentication (MFA) may also be referred to a 2-step or 2-factor authentication. This is a process that requires an additional validation step, alongside a password, to gain access to a system or service.

MFA may be used every time a user accesses a system, or when a user undertakes specific higher risk actions, such as logging in from a new device, changing a password, or transferring money.

MFA helps to protect services being compromised from theft or loss of passwords, or from cyber attacks that attempt to guess passwords.

LAA recommends that all email accounts and any IT system holding personal data is protected by MFA. Provider's should carefully consider the type of information stored in systems using single factor authentication (password only), whether that information is sufficiently protected from unauthorised access and the impact on the Provider, LAA or data subjects were that information to be lost or compromised.

4 – Additional Guidance

The LAA recommends the following guidance be adhered to, in support of the DSR.

4.1 Audit

The LAA may, at its discretion, audit compliance against the DSR as part of a contract compliance audit.

Auditing compliance will help to provide an independent and objective opinion about risks and what is being done to manage them. In line within normal audit protocols, Providers will be notified of the auditor's arrival beforehand and the audit scope will be agreed in advance.

Audits will review the way each Provider handles LAA's personal data consistent with the guidance contained in this document and identify any gaps in good practice and make recommendations. In addition to the standard audit assessments, spot checks may take place throughout the year to ensure that adequate controls are continually active and embedded into the Provider's business-as-usual activities. These checks may occur at short notice. These will be focussed at operational level compliance.

4.2 Policies

Email Policy

It is the responsibility of the Provider to have in place a robust email policy. Email should not be used as a system for the long-term storage of information. Emails should be drafted with care and marked OFFICIAL-SENSITIVE where necessary. Emails should be filed/stored where necessary to retain their contents or otherwise deleted. Emails should only be copied to those who need to know the information. Emails to the LAA may be disclosable in response to a freedom of information or subject access request.

Internet usage policy

All Providers must ensure that the use of internet services shall not introduce any material which would pose a threat to the reputation of the LAA, the security of LAA information or the integrity of LAA services. Further, no material shall be issued through the medium of the internet which shall cause a breach of security or which shall embarrass the LAA in any way. Personal data must always be encrypted before being sent over the internet.

There is a potential for external internet users to attack systems through the internet. There is also the possibility for staff to send, intentionally or unintentionally, malicious software or sensitive information over the internet.

All Providers should have an internet usage policy. The policy should ensure that all internet usage may be monitored at any time, and staff held to account for their usage. Misuse should have the potential to result in disciplinary and/or criminal action being taken. Users should be prevented from access to particular sites which may be sources of malicious software, pirated software or content in breach of UK law. All LAA Providers must adhere to the Computer Misuse Act.

Clear desk policy

It is best practice to ensure that when staff are absent from work stations or desks, documentation should be locked away. Whilst this may be impractical for short staff breaks or during meetings, it should be enforced for longer breaks, overnight and at weekends. Staff are expected to follow a clear desk policy.

Remote / Home Working policy

As set out in Requirement 5a Providers must have a remote/home working policy (where such working arrangements are authorised). This policy must set out the requirements of staff members to provide security for physical information assets kept at home, and security of access to electronic assets. This policy should provide for equivalent arrangements to those found in a Provider’s premise, including provision of lockable storage to which the staff member has exclusive access for storing paper documents or removable media containing personal data.

Remote Access

It is the responsibility of Providers with remote access privileges to their organisation’s corporate network to ensure that their remote access connection is given the same consideration as the user’s on-site connection to the organisation. Secure remote access is required to protect data so it can reviewed and amended without being permanently

stored on the remote computer. If this is the case, the following requirements must be followed:

- If the network is holding personal data or data classified as OFFICIAL then any remote access should be via IPSec or SSL Virtual Private Network (VPN) that has been implemented using a product that is certified as meeting the FIPS 140-2 standard;
- All computers connected to the internal networks via the VPN must use the most up to date anti-malware software and latest operating system patches;
- Where the network is accessed remotely via wireless, appropriate wireless security standards should be used. WPA-2 should be used as standard on Wi-Fi connections.

Remote access should be to a secure network owned by the provider. All Providers using remote access should have a remote access policy in place.

4.3 Preservation and Archiving

Effective file keeping methods must be in place in order for the organisation to comply with the LAA Record Retention and Disposition Schedule (RRDS) (available on gov.uk) and LAA audit requirements.

All Providers should implement processes to ensure that records are:

- Retrievable and traceable;
- Only retained as long as it is needed and in accordance with the LAA RRDS (for LAA Data) or professional duties/requirements on file retention and contractual requirements (for Shared Data);
- Stored appropriately with regard to the data sensitivity, in particular ensuring access is only given to authorised individuals that need access to the data;
- Appropriately disposed when the retention period has ended.

4.4 IT System Risk Assessments

Risk assessments must be conducted on all systems to ensure that they are robust and are running effectively, as well as ensuring that the data held on them is kept secure. Best practice suggests that these assessments should be updated on a quarterly basis and that all risks should be reported, logged and mitigated as soon as possible. All issues should be reported to a designated senior staff member with responsibility for the information asset (this may be referred to as the Information Asset Owner), as well as being logged on a risk register.

The DSR recommends that systems storing information relating to 100,000 or more identifiable individuals are subject to independent penetration testing. Such testing should identify risks to the system as well as assessing the adequacy of controls to mitigate known risks.

4.5 IT system audit logs

It is advisable for audit logs to be enabled on all systems so that faults and errors can be identified. Audit trails must maintain a record of system activity by system or application processes and by user activity. Audit trails can provide a means to help accomplish several security related objectives, including individual accountability, the reconstruction of events, intrusion detection and problem identification. These logs should be periodically reviewed, ideally monthly, as the system-generated logs can detect security problems, including attempts to exceed access authority or gain system access during unusual hours.

All Providers should enable audit logs on all systems containing personal data. Detailed arrangements for the retention periods of audit logs are a matter for individual Providers, but LAA recommends that audit logs should be retained for 6 months in a readily accessible, live or “on-line” form for instant querying and in an archive or “off-line” form for 2 years.

Annex 1 – Data Protection Principles

Article 5 of UK GDPR sets out 7 principles which lie at the heart of data protection.

Article 5(1) Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals (**Lawfulness, fairness and transparency**);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (**Purpose limitation**);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**Data minimisation**);

(d) accurate, and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**Accuracy**);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes subject to implementation of the appropriate technical and organisational measures required by UK GDPR in order to safeguard the rights and freedoms of individuals (**Storage limitation**);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**Integrity and confidentiality (the Security Principle)**).

Article 5(2) The Controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (**Accountability**).

Annex 2 – Data subject rights

Any living person whose personal data is being held by an organisation has the following rights under the DPA and UK GDPR.

- To know whether their data is being processed;
- To make a subject access request in writing to see any of their data held by that organisation, including the purposes for which it is held the source of the information and the types of organisation to which it may be disclosed;
- To have the data supplied to them in an intelligible form;
- To have any inaccuracies corrected or destroyed;
- To have their data held securely and not disclosed unlawfully;
- To prevent the processing of their data if that processing is likely to cause substantial and unwarranted damage or distress; and
- To claim compensation for loss and damage if their data is misused or wrongly disclosed.

Annex 3 – Government Security Classification System

The Government Security Classification[3] system (GSCS) has three levels.

The 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.

OFFICIAL
Summary - The majority of information that is created or processed by the public sector. This includes routine business operations 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.

This classification will apply to the vast majority of government information including general administration, public safety, criminal justice and law enforcement and 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.

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. The need to know principle must be rigorously enforced for this information, particularly where it may be being shared outside of a routine or well understood business process. This more sensitive information will be identified by adding SENSITIVE and must therefore be marked OFFICIAL-SENSITIVE. This marking alerts users to the enhanced level of risk and that additional controls are required.

Examples of information that the LAA has classified as OFFICIAL-SENSITIVE can be found below. Please note, this is not an exhaustive list.

OFFICIAL-SENSITIVE – casework examples

- Where there is a high media profile and risk of damaging unauthorised disclosure
- Witness protection cases
- Terrorism cases
- Serious and organised crime cases
- Serious, high impact or large scale fraud cases
- Special Immigration Appeals Commission (SIAC) cases
- Cases with an individual case contract
- Public Law Children Act cases
- ECF family cases involving risk of harm to children

[3] Government Security Classifications - GOV.UK (www.gov.uk)

- Forced Marriage Protection Order (FMPO) cases
- Applicants living in a refuge (specifically domestic violence cases)
- Where there is a specific risk assessment or threat to highly vulnerable individuals
- Cases involving intimidation and corruption

OFFICIAL-SENSITIVE – other examples

- Advice or documentation protected by legal professional privilege
- 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
- The most sensitive corporate or operational information, e.g. relating to organisational change planning
- Commercially sensitive pricing sets within contracts.

SECRET

Summary - Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.

Use of SECRET must only be used where there is a high impact and a sophisticated / determined threat. Examples include:

- Classified material received from other government departments / agencies relating to national security or counter-terrorism
- Intelligence and investigations relating to individuals of interest to security agencies
- Information that could seriously damage security and intelligence operations
- Information affecting the ability to investigate or prosecute serious and organised crime.
- Personal / case details where there is a specific threat to the life or liberty of an individual, such as protected witness scheme records.

The concept of sophisticated or heightened threat doesn’t only apply to those with a high technical (IT) attack capability but can apply to criminals who have developed capability to intimidate or coerce individuals i.e. if disclosure of information could result in serious physical harm or put a life at risk because there is a real and highly capable threat present, the information must be tightly controlled.

SECRET must not become the default status for material just because of the type of case or potentially severe consequences (e.g. murder trials, or where there is a threat to life). The threat capability must also be present.

Any Provider expecting to share information classified as SECRET must contact their Contract Manager beforehand to agree controls.

TOP SECRET
Summary - HM Government's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

This classification remains for information of the highest sensitivity relating to national security and subject to highly capable threat sources. There is no change to controls at this level. Any Provider holding or expecting to hold information at this level must contact their Contract Manager to agree controls.

Apply the Classification system
The following considerations apply:

- Providers are responsible for ensuring that all information is looked after with care to enable the business to function as well as meeting privacy needs.
- The majority of LAA and wider government information will fall into the OFFICIAL tier; there is a significant step up to SECRET and TOP SECRET which are essential for national security and the very highest threat areas.
- OFFICIAL provides for a general and sufficient level of control of information (including for IT systems holding such information) which is not subject to heightened threat sources. Within this, there is flexibility to apply additional operational controls to reflect sensitivity.
- Material at OFFICIAL will not require a marking to be applied, but must be protected in accordance with LAA instructions outlined in this document. However, information assessed to be particularly sensitive must be marked OFFICIAL-SENSITIVE, giving a clear warning that strict control of access and special handling may apply (see below).
- Providers are expected to comply with LAA instructions and minimum controls but need to exercise common sense when applying a control isn't possible or would seriously hinder effective business or safety. In all but the most urgent cases, seek approval from your Contract Manager before adopting lesser controls. Decisions must be risk based and the assessment must be recorded at the earliest convenient opportunity.
- Existing material with former protective markings (i.e. UNCLASSIFIED, PROTECT, RESTRICTED) does not need to be retrospectively reclassified.
- Descriptors such as PERSONAL or COMMERCIAL will no longer be routinely used, though in exceptional circumstances authors may include handling instructions in a document or email to draw attention to particular requirements.
- If you receive, handle or otherwise process any information at SECRET or TOP SECRET please contact your Contract Manager to agree controls.

Controls
Controls should be consistent with the minimum standards/requirements set out in this document. These must be applied to all information within OFFICIAL and will be adequate for most information, providing defence against the sort of threats faced by a major

organisation. Providers should review risks to their information and ensure local procedures are in place, adopting additional controls where needed.

Providers may decide to adopt more robust controls particularly for material marked OFFICIAL-SENSITIVE or where information is moved, transmitted or otherwise communicated outside of the secure office environment.

Controls should be applied proportionately for information which would previously have been UNCLASSIFIED. Such information will still need protecting to ensure the information's availability and integrity but may not require controls designed to provide confidentiality.

If Providers are handling SECRET or TOP SECRET information they should consult their Contract Manager to agree necessary controls.

Marking of Information
Marking is only needed for information which is OFFICIAL-SENSITIVE, SECRET or TOP SECRET.

It is important that documents are clearly marked as follows:

- At the top and bottom of documents, clearly, in CAPITALS and CENTRED (in the header and footer).
- Electronic document names should start with the marking (e.g. OFFICIAL SENSITIVE Statement of Case).
- In the subject line and at the top of emails:
    - Type OFFICIAL-SENSITIVE at the start of the subject line, in CAPITALS
    - Remember to consider whether material that is sensitive needs to be sent and whether it is safe or appropriate to send by email to this particular recipient, or group of recipients.
    - You must not email anything marked SECRET or above.
- Clearly on the front of folders, binders or bound case files
    - Apply in a prominent position, in CAPITALS
    - Apply the highest classification of any of the contents to the whole file

Material that needs marking must be transmitted securely. The classification of contents **must not** be visible on an external envelope sent by post or courier.

Annex 4 – Summary of Requirements and Compliance Record

Name of Provider:			Date of Review:		
	Requirement	**Mandatory / Recommended**	**Compliance (Compliant, Partial Compliance, Non-Compliance, N/A)**	**Evidence**	**Actions to Address Partial / Non-compliance**
1	Register as a Data Controller	Mandatory			
2	Appoint a Data Protection Supervisor	Mandatory			
3	Foster a culture that values and protects information	Recommended			
4	Maintain a level of staff awareness	Mandatory			
5a	Have a coherent set of policies	Mandatory			
5b	Have a coherent set of policies	Recommended			
6	Undertake an annual review	Mandatory			
7	Have in place an incident management policy	Mandatory			
8	Monitor and report	Recommended			
9	Implement a “whistle-blowing” procedure	Recommended			
10	Conduct Data Protection Impact Assessments	Mandatory			
11	Conduct staff screening	Mandatory			

12	Control access to personal data	Recommended			
13	Maintain access records	Mandatory			
14	Maintain adequate physical security	Mandatory			
15	Implement controlled disposal of records	Mandatory			
16a	Secure disposal	Mandatory			
16b	Secure disposal	Recommended			
17	Conduct formal, documented, risk assessments	Recommended			
18	Apply appropriate controls	Recommended			
19	Cyber Essentials Plus	Recommended			
20	Conduct independent penetration testing	Recommended			
21	Ensure business continuity	Mandatory			
22a	Hard disk encryption	Mandatory			
22b	Hard disk encryption	Recommended			
23a	Encryption of removable media	Mandatory			
23b	Encryption of removable media	Recommended			
24	Encryption of personal electronic devices	Mandatory			
25	Regular encrypted backup	Recommended			
26	Secure transfer	Recommended			
27	Malware protection	Mandatory			
28	Multi-factor authentication	Recommended			