Legal Aid Agency

Legal Aid Agency – Information Security

Handling Personal Data and Documents Data Security Guidance

November 2020

Table of Contents

AMENDMENT POLICY

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

Changes Made to the 'Handling Personal Data and Documents – Data Security Guidance' – April 2014

Paragraph Number in April 2014 document	Changed From	Changed To	Comments

General	Legal Services Commission (LSC)	Legal Aid Agency (LAA)	All references to LSC have been updated to LAA throughout the document. The format of the document has been improved to aid the reader. References to 'protective marking' and the Government Protective Marking Scheme have been removed and replaced with the new Government Security Classification system (GSC), where relevant.
Table of Contents			Improved to aid the reader.
Table of Referenced Documents			The table has been updated quoting the latest versions of the referenced documents.
2.1 - Overview		[INSERTION] Also relevant to barristers are the 'Guidelines on Information Security' on the Bar Councils website: http://www.barcouncil.org.uk/forthebar/professionalpracticeand-ethics/itpanelarticles/guidelinesoninformation-security/	Updated to reflect Bar Council's Guideline on Information Security.
2.2 LAA Contracts	[REMOVED] The Legal Services	[INSERTION] All contracts include specific requirements	Reference to the Access to Justice Act

	Commission (LSC)		(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).	for preserving the security of the information Providers receive from LAA and also share with the LAA.	this is no longer relevant.
Protected Personal Data (was paragraph 2.7 in April 2012 version).	Under the Government Protective Marking Scheme (GPMS), the Government has implemented a category of information referred to as "PROTECT: PERSONAL DATA". **All Personal and Sensitive Data relating to the work undertaken for LSC contracts should be marked "PROTECT: PERSONAL".**		This paragraph and requirement has been removed, as the Government Protective Marking Scheme (GPMS) is no longer in place. The Government Security Classification system has replaced GPMS and only requires personal data to be marked by exception. Guidance on the new Government Security Classification system is outlined in section 4.1.2 and in appendix 3.
3.1 Roles and Responsibility	Roles and responsibilities diagram removed.		
3.2 Information Assets			The definition of an information asset has been updated to provide clarity.

4.1.2	All references to marking personal data PROTECT-PERSONAL has been removed.	Sub- heading re- titled to: 'Classifying and marking date – The Government Security Classification system' [INSERTION] - New section on the Government Security Classification system.	Informs the reader that personal data falls within the OFFICIAL classification and only exceptionally sensitive data within the classification should be marked, as OFFICIAL SENSITIVE. The reader is directed to further guidance in Appendix 3.
5.1.1 – IT system risk assessments		[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. Req. 24 – Conduct independent penetration testing – Recommended – Independent penetration testing of systems that store process or transmit information relating to 100,000 or more identifiable individuals.	.
4.4.3 (Nov 2020)		No data may be transferred outside of the EEA without prior written authorisation from the LAA	Line added to clear inconsistency and for clarification

2.6 (Nov 2020)	DPA 1998 definition of 'special categories of personal data'	DPA 2018 definition of 'special categories of personal data'	Definitions have changed slightly since the new Act came into force
4.7.3 (Nov 2020)		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 UK and the EEA.	Added for clarity and to ensure data is not sent outside the UK and the EEA

Apprendix (Nov 2020)	8 principles of the Data Protection Act	7 principles of the GDPR	
Entire document (Nov 2020)	EU GDPR	UK GDPR	To reflect changes to UK legislation as a result of Brexit
Appendix 3		[INSERTION] Government Security Classification system Guidance.	
Appendix 4 – Summary of Requirements and Compliance Record		[INSERTION] - Req. 24 - Conduct independent penetration testing – Recommended.	

REFERENCED DOCUMENTS

The following is a list of documents with a direct bearing on the content of this report. Where referenced in the text, these are identified as Ref. n where 'n' is the number in the list below:

Ref.	Title	Date / Version	Author
1.	Data Security Requirements	V.2 - April 2014	Legal Aid Agency
2.	Data Protection Act	2018	HMSO
3.	HMG Security Policy Framework (SPF) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework__web__April_2014.pdf	V11 - October 2013	Cabinet Office
4.	ISO 27001	2005	International Standards Organisation
5.	ISO 27002	2005	International Standards Organisation
6.	UK General Data Protection Regulations https://ico.org.uk/for-organisations/guideto-data-protection/guide-to-the-generaldata-protection-regulation-gdpr/principles/		

1 Scope of this document

The nature of the services provided by the Legal Aid Agency (LAA) through Civil Legal Aid and Criminal Legal Aid 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 unauthorised or unlawful processing, accidental loss, destruction or damage and to maintain the confidentiality, integrity and availability of information.

The contracts between LAA and the Providers refer to two documents:

- Data Security Requirements [Ref. 1];

[1] A 'Provider' means a party (except LAA) to a contract with LAA in respect of the provision of legal services funded by LAA

- Data Security Guidance [This document];

The Data Security Requirements [Ref. 1] sets out the mandatory and desirable requirements. This document sets out the Data Security Guidance referenced in the contracts between LAA and the Providers.

The intention of this document is to make all Providers involved in the administration of Legal Aid aware of the policy, principles and requirements that govern the obtaining, use, storage and destruction of "**Personal Data"** (defined below).

This document explains what the Providers' (including their employees and any third parties they appoint in accordance with the contract) responsibilities are under the **Data Protection Act 2018** ("the DPA"), UK General Data Protection Regulations (UK GDPR) and the relevant section of the HMG Security Policy Framework (SPF) [Ref. 3] and its supporting documents.

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 Data Security Requirements to any third parties appointed by Providers.

If we authorise you to perform Remainder Work the terms of this Contract will, in respect of such Remainder Work, continue in full force and effect. This includes using your best endeavours to comply with the Data Security Requirements and having regard to this Data Security Guidance.

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

All Government Departments and Providers handle 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 Departments and Providers’ responsibilities towards that data. This document is based around **HMG Security Policy Framework** [Ref. 3] and its supporting documentation, the data protection requirements and security good practices set out in ISO 27001 [Ref. 4] and ISO 27002 [Ref. 5].

The SPF states:

All information that HMG deals with has value. HMG handles the wide variety of information that it generates, collects, processes, stores and exchanges appropriately to ensure: the confidentiality of citizen data and commercial information; good government and the effective and efficient delivery of public services; the proper protection of national security-related information; and that obligations to international partners are met. HMG expects its’ partners in the wider public sector, suppliers and other commercial partners who handle information on HMG’s behalf to do the same. Also relevant to solicitors’ practices is the information security and data protection guidance on The Law Society’s website:

- http://www.lawsociety.org.uk/advice/practice-notes/information-security/

Also relevant to barristers are the “Guidelines on Information Security” on the Bar Council’s website:

- http://www.barcouncil.org.uk/for-the-bar/professional-practice-and-ethics/itpanelarticles/guidelines-on-information-security/

2.2 LAA Contracts

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

The Data Security Requirements [Ref. 1] 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 Data Security Requirements document and then sets out more information about the types of actions that Providers are expected to carry out in order to meet those requirements.

2.3 Culture

The Data Security Requirements document [Ref. 1] requires Providers to:

Req 1	Foster a culture that values and protects information	Mandatory	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 7 General Data Protection Principles

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.

2.4 Handling Data

The Data Security Requirements document [Ref. 1] requires Providers to:

Req 2	Control access to personal data	Mandatory	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 job role

The LAA is responsible for handling the data in a secure manner once it has been received from the Providers, but this document sets out the policies and procedures that should be followed to preserve the security of the data that is going to be sent to LAA and may be received back from LAA.

2.5 Definition: Personal Data

The DPA defines “Personal Data” as data relating to a living individual (otherwise known as the Data Subject) who can be identified either from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller. Whilst the DPA refers to living individuals, the principles in this document also apply to deceased individuals and their records.
In addition, the individual 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 indication of the intentions of the data controller or any other person in respect of the individual.

The following list provides examples, relevant to the work of LAA, of the types of Personal Data which may be held:

- Parties involved in a case ✦ The parties’ names and addresses
- The merits of a case
- Details of a case
- Information required to judge the merits of a case
- Contributions made by parties
- Fee schemes that apply to a case
- Bills and payments
- Customer service information
- Date of Birth
- National Insurance Number (NINO)

This list is by no means exhaustive and can cover information which could cause harm if released, such as the current addresses of some of the parties involved in a case.

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

2.6 Definition: Special Categories of Personal Data

The DPA identifies an additional set of Personal Data which is particularly sensitive and can only be processed in certain limited circumstances (for example, with the consent of the individual concerned, or if employment law imposes a specific obligation to carry out the processing).

In the Data Protection Act “sensitive personal data” means personal data consisting of information as to:

(a)the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b)the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

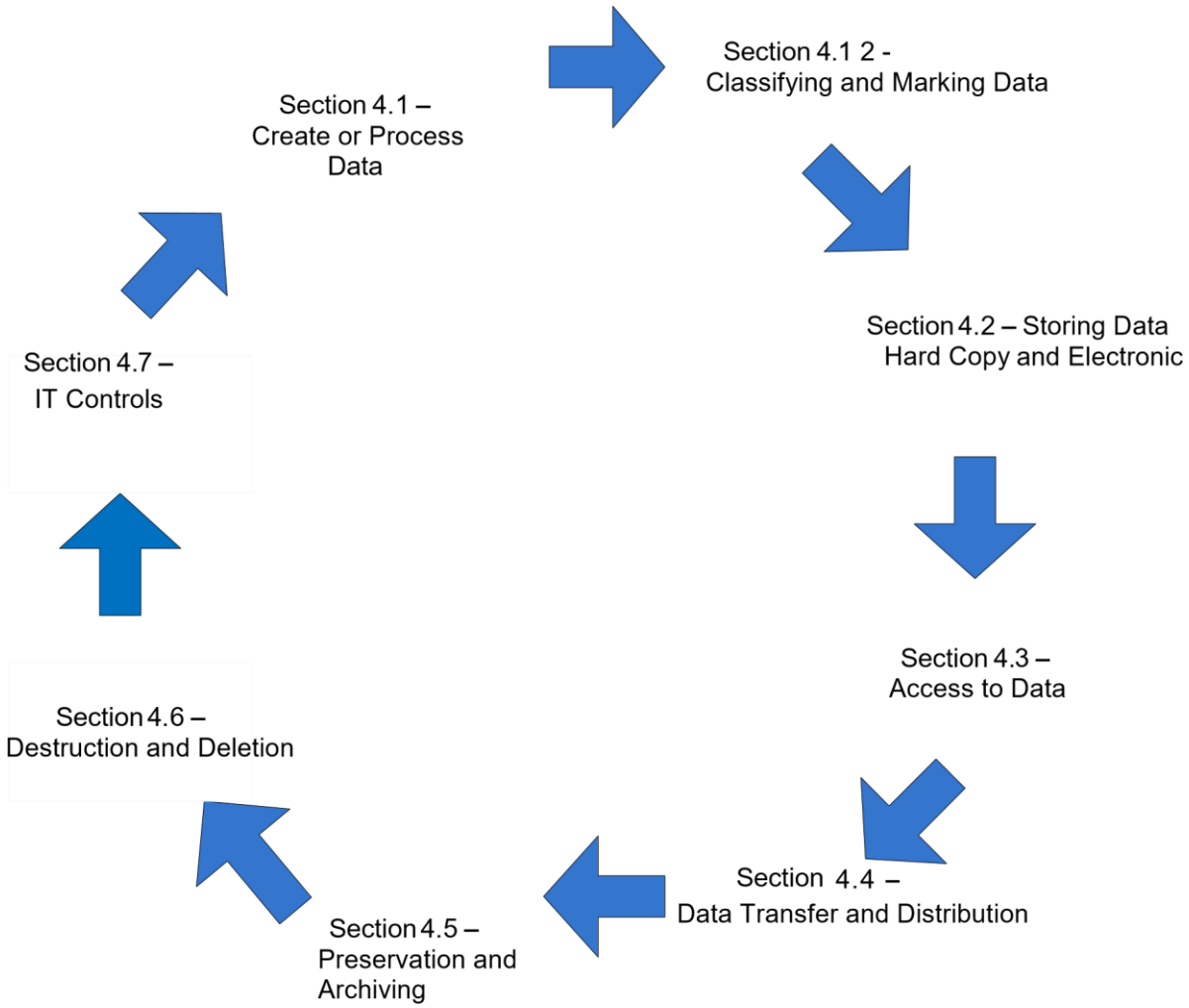
(c)the processing of data concerning health;

(d)the processing of data concerning an individual’s sex life or sexual orientation. In the context of Legal Aid work, Sensitive Personal Data may also include the following:

- The details of a case
- The merits of a case.

2.7 Data handling cycle

Providers should be aware of key processes involved in managing LAA hard copy and electronic data. **Section 4** of this document sets out the technical requirements for each of the areas identified. The data cycle below shows the main phases from creating data through to final destruction or deletion. Providers should consider all phases within their Data Handling Policy to ensure that the requirements of data handling are met in each phase.



3 Governance

3.1 Roles and Responsibility

The Data Security Requirements document [Ref. 1] requires that Providers have the following measures:

Req 3	Register as a Data Controller	Mandatory	To be registered as a Data Controller with the Information Commissioner's Office, unless an exemption applies
Req 4	Appoint a Data Protection Officer	Mandatory	Appoint a senior member of staff as a Data Protection Officer with overall responsibility for data protection and information security

The term Data Controller is defined within the Data Protection Act 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 Officer is used in these documents to refer to the specific individual with responsibility for data protection and information security within the Providers' organisations.

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 help enhance the processes by which organisations understand and manage their information risk.

3.2 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/document or a set of related data, documents or files; it can be shared or be confined to a specified 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 only in hard copy. This guidance applies equally to both types.

3.4 Recruitment and Staff Vetting

The Data Security Requirements [Ref. 1] states that Providers are required to:

Req 5	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 Providers employ 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 Register; and ✦ Checks with the Criminal Records Bureau.

3.5 Training and Awareness

Under the Data Security Requirements [Ref. 1], Providers are required to:

Req 6	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 to comply with policies and procedures.

In order to ensure that all Providers meet their data handling requirements, it is 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 should:

- 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 it has a consistent approach to training; and
- Cover obligations relating to Data Protection, IT security, records management and privacy education, and;
- sessions should highlight key policies and procedures and give individuals the chance to ask questions and receive clear advice related to their function;
- be regularly refreshed and not just a one off; and
- Maintain content and version control for information security and privacy training materials, and make these available for audit inspection if required.

3.6 Audit

The Data Security Requirements [Ref. 1] states that Providers are required to:

Req 7	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 the audit trail for compliance with policies
Req 8	Monitor and report	Recommended	Monitor compliance with data protection and security policies and produce annual audit report

To ensure that Providers are following good standards and guidelines and given its commitment to enhancing the transparency of action in relation to the security of data, regular reviews may take place. These assessment/reviews will help to identify weaknesses, which in turn can be rectified.

Auditing compliance will help to provide an independent and objective opinion about risks and what is being done to manage them. In line with 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 with good practice recommendations for those who would be responsible for mitigating them.
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

organisation's business-as-usual activities. These checks may occur at short notice. These will be focussed on operational level compliance.

3.7 Risk Management

The Data Security Requirements document [Ref. 1] recommends that Providers:

Req 9	Conduct formal, document risk assessments	Recommended	Conduct formal, documented risk assessments for all systems that store, process or transmit personal or sensitive information when systems undergo significant changes, or at least every 5 years
Req 10	Apply appropriate controls	Recommended	Risk assessments must identify the assets, analyse and evaluate the risks to the 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/EC 27001, additional controls and control objectives may also be selected.
Req 11	Conduct Privacy Impact Assessments	Recommended	Where appropriate, conduct Privacy Impact Assessments of any new system developments or projects, using the Data Protection Impact Assessments for guidance (at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

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 must identify, manage and take actions to mitigate any risks surrounding the production, storage, use, transfer, destruction and deletion of records and data. This includes:

- Regular reviews for all processes and procedures;
- Business impact assessments; and
- Checks to confirm how robust the processes in place are in 'business as usual' situations.

3.8 Data Handling Policy Document

Under the Data Security Requirements document [Ref. 1] Providers are required to:

Req 12a	Have appropriate organisational and technical measures to adhere to the data protection principles	Mandatory	• Information Risk Management • Data Protection Compliance • IT security which includes an acceptable Use Policy that outlines the type of behaviour expected from staff when using technology in the workplace and the consequences for abusing technology privileges • Compliance with the current Government Security Classification (GSC) system
Req 12b	Have a coherent set of policies	Recommended	• Clear desk policy • Information Security, to include restricting use of portable media (e.g. USB memory sticks, discs, laptops etc). • HR standards that reflect performance in managing information risk and complying with above policies, incorporating sanctions against failure to comply
Req 12c	Undertake annual review	Mandatory	Supporting procedures and to conduct an annual review of the effectiveness of the policy or policies

To ensure good data handling practices, all Providers should have a Data Handling Policy in place, which as a minimum meets the following requirements:

- Documented processes/procedures describing data handling activities;
- Is reviewed and updated regularly (at least annually) to ensure it remains up to date;
- Is distributed, in at least summary form to all staff at least annually;
- Is made easily accessible to all staff and employee/Providers and is specifically drawn to the attention of all new staff; and
- Conforms 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 3.2 are run in line with best practice as detailed in this standard.

Further details on the content of the Data Handling Policy Document can be found in Section 4 of this document.

3.9 Incident Management Process

All Government Departments are required to have an active incident management process in place, which gives clear guidance on how individuals can handle live incidents such as lost personal data, computer viruses, other malicious codes, human errors or system intruder (internally or externally).

The Data Security Requirements [Ref. 1] states that Providers are required to:

Req 13	Have in place an incident management policy	Mandatory	Have a policy for reporting, managing and recovering from information risk incidents, including losses of personal data and ICT security incidents, defining responsibilities, and make staff aware of the policy

The Provider's **Data Handling Policy** should document the procedures.

All Providers should have an **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 information and communication technology ("ICT") security incidents;
- Confirmation that the Provider will inform LAA, via their Account Manager, within **1 working day** of becoming aware of a loss of data or suspected security breach of any kind , and then follow the instructions received from LAA;
- A statement that all staff should provide details of **the exact nature** of any such data security breach to the LAA
- Confirmation that the Provider will take all responsible action to prevent the future loss of data.

Once an incident has been reported it would be followed up using the same procedure that is in place for dealing with any reports of breaches internally within the LAA. It is also important to note that certain breaches should be reported to the Information Commissioner's Office. Guidance on this can be found at: https://ico.org.uk/for-organisations/guide-to-eidas/breach-reporting/ .

4 Technical Requirements

All the practical steps set out below should be included within the Provider's **Data Handling Policy**. When completing the Data Handling Policy, Providers should consider the 3 phases below and the requirements within each phase as well as the data handling cycle.

4.1 Creating / Re-processing and Marking Data

4.1.1 Creating and re-processing data

This section is about classifying data in order to ensure that the data is handled correctly to reflect the requirements of that data.

In the work that Providers are completing, there may be a requirement to both create new data and documents and to re-process data or documents. In both circumstances the Provider must appropriately classify the data/document along with any media the data is being sent on or by.

4.1.2 Classifying and marking data – The Government Security Classification system

In April 2014, the Government introduced the Government Security Classification system (GSC). This replaced the Government Protective Marking Scheme (GPMS). The GSC system has a three-tier system to indicate how to handle information. The classifications are:

- **OFFICIAL**
- **SECRET**
- **TOP SECRET**

The vast majority of LAA Sensitive and Personal Data relating to work undertaken for the LAA Contracts should be classified as OFFICIAL. This includes most legal aid applications, case files and claim information.

Most information classified as OFFICIAL does not need to be marked. Under GPMS the requirement was to mark personal information, 'PROTECT – PERSONAL'. This no longer applies. However, the requirement to ensure that the information is protected and only shared with those that need to know still applies.

There is, however, some information within OFFICIAL that will be especially sensitive. This **must** be marked, 'OFFICIAL-SENSITIVE'.

OFFICIAL-SENSITIVE should be used **by exception** in limited circumstances where there is a **clear and justifiable requirement** to reinforce the 'need to know principle' as compromise or loss could have **damaging consequences** for an individual (or group of individuals), the LAA or Government more generally.

For detailed information on the GSC system including the types of information which the LAA has classified as 'OFFICIAL SENSITIVE' and how to mark and handle this information, please see Appendix 3.

4.2 Storing Data

4.2.1 Physical security

The Data Security Requirements [Ref. 1] states that Providers must:

Req 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

4.2.2 Electronic data storage

If the files are in an electronic format then security controls should be in place such as password protection; access restriction on the system; and/or encryption.

4.2.3 Electronic storage devices and encryption

The Data Security Requirements [Ref. 1] state the following:

Req 15a	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
Req 15b	Hard disk encryption	Recommended	It is recommended that the hard disc encryption product is compliant to FIPS-140 standard
Req 16a	Encryption of removable media	Mandatory	All portable devices (e.g. USB memory sticks, external hard drives) used to store personal or sensitive information shall be protected by using encryption
Req 16b	Encryption of removable media	Recommended	It is recommended that the encryption used is AES encryption of at least 128-bit strength

All Providers must ensure that the use of external storage devices is kept to a minimum and if possible not used at all. Storage devices such as USB sticks should **never** be used to carry important documents – they should only be used as a temporary data store for duplicate files and used in a highly controlled way with encryption. All Providers must ensure that any electronic records transferred to removable media devices such as CDs or USB sticks are encrypted to a standard of at least **FIPS 140-2** or equivalent, in addition to being protected by an authentication mechanism, such as a 'strong' (i.e. one that is not easy to guess or crack) password.

All Providers must ensure that information stored in any web based system is stored in such a fashion that access is limited to authorised individuals and that any information transferred to a third party or backed-up is encrypted.

4.2.4 Hard copy storage

It is important to ensure that all documents containing Personal Data are placed in locked cupboards or drawers when they are not in use. If files containing Personal Data are in a hardcopy format then they should be marked if they contain OFFICIAL-SENSITIVE information, and kept within a locked cabinet with access to the cabinet carefully controlled.

4.2.5 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.

4.3 Access to Data

4.3.1 Access rights and access levels

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

Providers must conduct regular **user access right reviews** to ensure:

- That all users who have access to the system are authorised to handle the data;
- That individuals have the correct access privileges in accordance with their job roles e.g. the users have not been given excessive access rights to the system;
- That all users who have left the organisation or no longer need access to the system are identified and removed from the system as soon as possible; and
- That all users with administration rights are checked to see if they have a justifiable reason for having these privileges.

4.4 Data Transfer and Distribution

Everyone should be made aware of the dangers of sending hard copy and electronic data. Before sending any item, Providers should question what information is being sent and the method it should be sent by to enable safe and secure delivery. They should also take into account the volume of data to be sent in a single package.

4.4.1 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’, secure Document Exchange (DX) or via an internal van service specific to that contractor. Use of these services means that, if required, progress in delivery can be tracked and traced. Records or data must be in a sealed envelope. Other

regular postal distribution involving multiple parties and Personal Data should be agreed with LAA.

All Providers must ensure that all media devices/data are encrypted to the FIPS 140-2 standard before they are sent. Providers should ensure that as a minimum, either the data file or the media is encrypted to the relevant standard. The content of data drives etc should not be readily identified without prior knowledge of the content.

4.4.2 Sending data electronically

By using approved encryption techniques, the risks of unauthorised interception are minimised.

The Data Security Requirements [Ref. 1] states that Providers must ensure:

Req 17	Secure transfer	Recommended	Appropriate protection must be provided to protect the confidentiality, integrity and availability of personal or sensitive information transferred from one physical location to another or transmitted electronically

Data being exchanged with LAA information systems is protected by the use of Secure Sockets Layer (**SSL**).

In some circumstances, the LAA will exchange data with Providers by email. In those circumstances LAA will encrypt relevant emails containing Personal Data or Sensitive Data. The main mechanism for exchanging emails securely with Providers is the Criminal Justice Secure Mail (**CJSM**) system. Further details about CJSM and a link to a page for submitting an application to use the service can be found at:

https://www.cjsm.net/

Whilst use of CJSM is not mandatory, it is recommended that all providers subscribe to this service.

4.4.3 Sending data overseas

Data that is sent overseas must conform to Section 18 of the Data Protection Act and Articles 44 to 50 of the 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 LAA's prior authority. When sending data abroad, the level of encryption (of at least FIPS 140-2 or equivalent in addition to being protected by an authentication mechanism, such as a password that is not easy to crack) employed will 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 LAA on a suitable method of transfer. Before sending data overseas, LAA 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 to the level of protection afforded to the information when it is in the UK.
- Confirmed that they have followed the principles and guidance around Article 44 of the UK GDPR https://ico.org.uk/for-organisations/guide-to-dataprotection/guide-to-the-general-data-protection-regulation-gdpr/internationaltransfers/
- 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 the data; and
- Obtained written approval from the LAA Information Asset Owner (IAO)

In addition, consideration needs to be given to whether the data subjects need to be informed that their data may be transferred cross-border.

4.5 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.

All Providers should make sure processes are in place to ensure that records are:

- Retrievable and traceable;
- Only retained as long as it is needed and in accordance to the LAA Record Retention and Disposition Schedule policy;
- Stored appropriately with regard to the data sensitivity (i.e. stored so that access is restricted to authorised individuals and cannot be easily forced by unauthorised individuals); and
- Appropriately disposed of when instructed (See Section 4.6).

4.6 Destruction and Deletion

The DPA states within its fifth principle that “data shall not be kept for longer than is necessary”. The LAA Record Retention and Disposition is available to help ensure that all documents are destroyed in a timely manner. LAA will direct Providers regarding retention periods. Destruction will be in line with legal requirements (including any professional requirements mandated by professional bodies e.g. the Law Society) to retain information and the agreed retention schedule.

The Data Security Requirements [Ref. 1] states that Providers must:

Req 18	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.

4.6.1 Electronic copy deletion

As soon as the electronic file reaches the end of its retention period, it should be deleted in such a way that it cannot be retrieved by simply undoing the last action or restoring the item from the recycle bin.

Any magnetic media such as CD/DVDs must be completely destroyed via disintegration, pulverisation, incineration or shredding.

When no longer required, all references to that data should be removed from the system.

4.6.2 Hard copy destruction

There are several ways in which documents should be destroyed:

- Shredding - Shredders can be used to destroy Personal Information that is no longer required. These should cross-cutter shredders with a very fine cut, but shredding paper into ribbon is not approved;
- Confidential waste – Paper with personal data and all material classified as OFFICAL-SENSITIVE which is no longer required, should be placed in confidential waste. This waste should be kept secure until final disposal via shredding or incineration.

All Providers must ensure that all hard copy records and data are destroyed in line with the LAA Record Retention and Disposition policy. All sensitive hard copy documents much be destroyed via shredding or the use of approved confidential waste arrangements. The Data Security Requirements [Ref. 1] states the following:

Req 22a	Secure disposal	Mandatory	Dispose of electronic media holding LAA data through secure destruction
Req 22b	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 upon permanent disposal

4.7 IT Controls

4.7.1 Laptops

Where Providers are using laptops, the following security must be in place:

- All Laptops must have installed encrypted hard-drives. Preferably this encryption should be to the FIPS 140-2 standard; and
- Once a laptop is finished with, arrangements must be made to wipe data securely to the relevant Government standard (contact LAA On-Line Help Desk if more specific guidance is required).

4.7.2 Personal Electronic Devices (PEDs) Digital Assistants (PDA) devices

Personal Electronic Devices (PEDs) include Personal Digital Assistants (PDAs), tablets, smart phones, etc.

PEDs, by virtue of the data stored within them, must be given the same physical security protection given to other information assets. Where Providers are using PED devices, the following security must be in place:

- PED use must be kept to a minimum;
- No Personal Data should be stored on the device;
- PEDs must be password protected;
- PEDs must have the ability to lock the device or erase its contents after a predetermined number of failed password attempts;
- Anti-virus software must be installed on the PED;
- PEDs must be encrypted; and
- PEDs must be disposed of securely. The disposal procedures must ensure that either:
- All data is effectively wiped from the device; or
- All removable memory/media is destroyed, the Device is reformatted and the operating system software is re-installed.

Where a PED is in use and does not comply with the Departmental specification only nonsensitive data may be stored on it, such as calendar events and contacts.

4.7.3 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 be 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 information 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 certified as meeting the FIPS 140-2 standard;
- All computers connected to the internal networks via VPN must use the most upto-date anti-virus software and operating system patches; and
- Where the network is accessed remotely via wireless, appropriate wireless security standards should be used. Wireless Application Protocol 2 (WPA-2) should be used as standard on Wi-Fi connections.

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.

All Providers should have a remote access policy in place.

4.7.4 Anti-Malware policy

Anti Malware Policy includes not only viruses by also Trojan Horses, worms, etc, Viruses are one of the most prevalent forms of attack on computers. They may enter the system from a number of sources, but disks and e-mail attachments are the most common.

The Data Security Requirements [Ref. 1] state that Providers must have:

Req 19	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

If a virus is detected or just suspected because your workstation is behaving oddly, the following actions should be carried out immediately to prevent the spread of infection elsewhere:

- Stop using your workstation and switch-off. (Under no circumstances restart the operating system or power-on the workstation without the presence of the Local Administrator.);
- Inform the Local Administrators and preserve as much evidence as possible (e.g. suspect removable media, details of e-mail);
- Until the Local Administrator says you can resume use of your workstation, place a “DO NOT USE” notice on it and inform everyone to whom you have sent e-mail attachments or given information on removable media;
- Your organisation may have its own policies and procedures that should be followed to prevent viruses from getting onto the information systems. Where available, these should also be followed provided that they do not contradict the requirement expressed above.

4.7.5 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, marked OFFICIAL-SENSITIVE, where appropriate, and filed if required for long term retention or otherwise deleted as soon as possible and must only be copied to those who need to know the information. Emails may be liable to be disclosed in response to a request under the Data Protection Act or the Freedom of Information Act.

All Providers should have an email policy in place.

4.7.6 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. The LAA acknowledges that arrangements to meet this requirement will need to be subject to further discussions.

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 out over the Internet. Therefore, Providers' policy should ensure that all Internet usage may be monitored at any time, and staff held to account for their usage. Misuse may 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 information in breach of UK or EU law. All LAA Providers must adhere to the Computer Misuse Act.

All LAA Providers should have an internet usage policy.

5 System Requirements

5.1 Back-end IT System Controls

5.1.1 IT system risk assessments

The SPF states that risk assessments must be conducted on all systems (including the core Information Assets) 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 identified should be reported, logged and mitigated as soon as possible. All issues should be reported to the Providers' IAO equivalent, as well as being logged within the Provider's risk register.

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.

The Data Security Requirements [Ref. 1] states that Providers should:

Req 24	Conduct independent penetration testing	Recommended	Independent penetration testing of systems that store, process or transmit information relating to 100,000 or more identifiable individuals

5.1.2 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 as the system-generated logs can detect security problems, including attempts to exceed access authority or gain system access during unusual hours. LAA recommends that audit logs should be retained for 6 months on-line for instant querying and for 2 years off-line.

All Providers should enable audit logs on all systems containing Personal Data. Detailed arrangements for the duration of how long audit logs are retained are a matter for individual Providers, but the policy must be provided to LAA. To enable any issues to be identified and

corrected these logs should be reviewed at least once every month and any issues identified should be recorded and corrected.

5.1.3 System backups

All systems and services with Personal Data must be backed up regularly.

The Data Security Requirements [Ref. 1] states that Providers should:

Req 20	Regular encrypted backup	Recommended	Back up of all data daily, as required. Particular care must be taken to ensure the physical security of any unencrypted backup media

All Providers should have a clear written backup procedure and secure mechanisms in place to ensure that the data is secure at all time (when the data is being transferred and where it is stored). All back-up 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 back-ups should be tested at least annually. Providers must ensure that any Personal Data is not retained for any longer than required as stated in the DPA. Providers must be able to retrieve information from back-ups if required.

5.1.4 Business continuity

The Data Security Requirements [Ref. 1] states that Providers must have:

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

All Providers should have plans in place that will enable them to resume service within a day of a disaster affecting their buildings or information systems.

The plans should ensure that the security of information that they handle is maintained.

The plans should be tested to ensure that they can operate as they are expected to, and to help restore service within an acceptable timeframe.

Appendix One

The 7 Data Protection Principles are as follows:

Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that 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 the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(b) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(c) 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');

(d) 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 the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(e) 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').

Attached is a link to the Data Protection Act 2018:
https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Appendix two

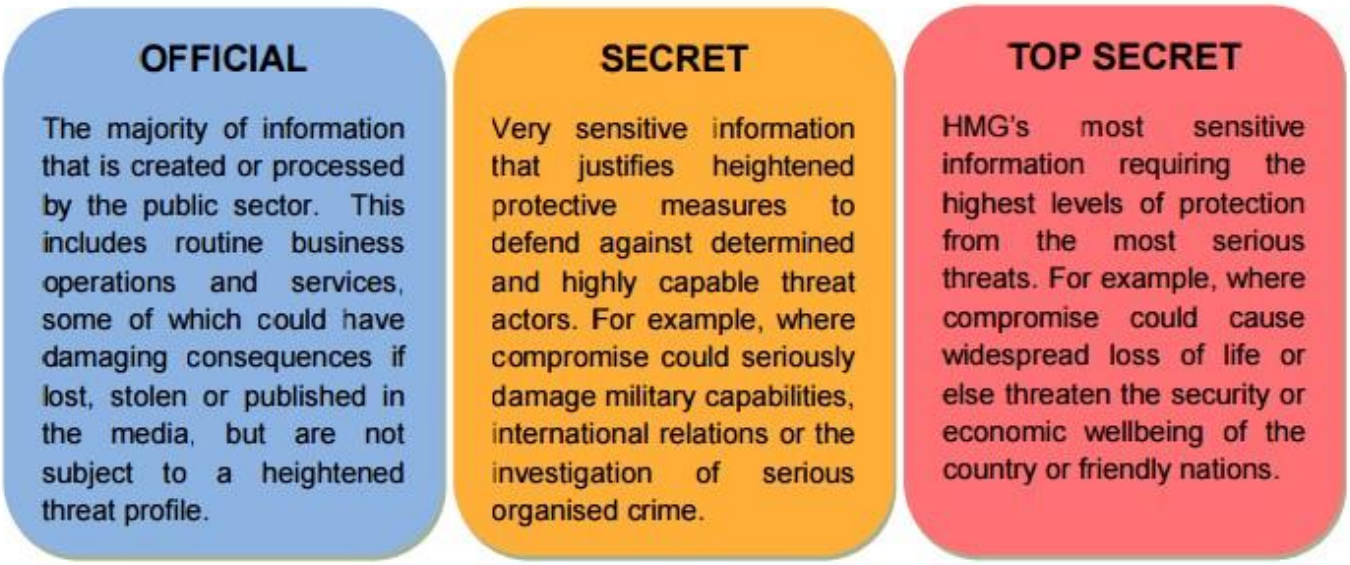
Any living person whose personal data is being held by an organisation has the following rights under the DPA:

- 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 disclose.

Appendix three

The Government Security Classification system (GSC) has three levels: OFFICIAL, SECRET and TOP SECRET.

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. There are three levels of classification:



OFFICIAL

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.

OFFICIAL - SENSITIVE

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.

Casework

- Where there is a high media profile and risk of damaging unauthorised disclosure
- Witness protection cases
- Terrorism charge cases
- Serious and organised crime cases

- Serious/high impact/large scale fraud
- Special Immigration Appeals Commission cases (SIAC)
- Cases with an individual case contract
- Public Law Children Act cases
- ECF family cases involving risk of harm to children
- Forced marriage protection order 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 **Other information**
- 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
Use of SECRET must only be used where there is a high impact and a sophisticated / determined threat (elements of serious and organised crime and some state actors):

- Classified material received from other government departments/agencies relating to national security and counter-terrorism.
- Intelligence and investigations relating to individuals of interests to security agencies.
- Information that could serious damage security and intelligence operations.
- Information affecting the ability to investigate or prosecute serious/organised crime.
- Personal/case details where there is a specific threat to the life/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 a 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 at this level must contact their Contract Manager beforehand to agree controls.

TOP SECRET
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 Team to agree controls.

Applying 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 ICT 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 the 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 Information Asset Owner 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 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 handling controls.

Controls

Controls should be consistent with the minimum controls 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 company. These threats include (but are not limited to) hacktivists, single issue pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups.

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 looking after if it is needed to do the job, but may not require controls designed to provide confidentiality.

If Providers are sharing SECRET or TOP SECRET information with the LAA, 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 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 OFFICIAL-SENSITIVE
- 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 to the recipient
    - You must not email anything at 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.

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.

Appendix 4 – Summary of Requirements and Compliance Record

The Data Security Requirements [Ref. 1] document states that Providers should

Req 8.	Monitor and report	Recommended	Monitor compliance with data protection and security policies and produce annual audit report

The Data Security Requirements [Ref. 1] document also recommends that Providers should consider:

Req 23	Implement a 'whistleblowing' procedure	Recommended	Implement mechanisms for raising concerns about information security or any incidents of breaches of the Act or related policies

To assist in meeting this requirement all Providers should complete the compliance matrix below stating whether they are fully compliant, partially compliant or non-compliant with the requirement for handling

Personal Data. Providers should document evidence to demonstrate full or partial compliance and set out the actions proposed to address partial or non-compliance. Please note that not all the requirements will be applicable to all Providers.

Dd mmm 20nn Compliance Statement		
Name of Provider:	**Data Protection Supervisor:**	**Date:**

	Requirement	Mandatory / Desirable	Fully Compliant, Partial Compliant, Non-Compliant (please note where this is N/A)	Evidence	Actions to address partial or non-compliance
1.	Foster a culture that values and protects information	Mandatory			
2.	Control access to personal data	Mandatory			
3.	Register as a Data Controller	Mandatory			
4.	Appoint a Data Protection Supervisor	Mandatory			
5.	Conduct staff screening	Mandatory			
6.	Maintain a level of staff awareness	Mandatory			
7.	Maintain access records	Mandatory			
8.	Monitor and report	Recommended			
9.	Conduct formal, document risk assessments	Recommended			
10.	Apply appropriate controls	Recommended			
11.	Conduct Privacy Impact Assessments	Recommended			
12a.	Have a coherent set of policies	Mandatory			
12b.	Have a coherent set of policies	Recommended			
12c.	Undertake annual review	Mandatory			
13.	Have in place an incident management policy	Mandatory			
14.	Maintain adequate physical security	Mandatory			
15a.	Hard disk encryption	Mandatory			
15b.	Hard disk encryption	Recommended			
16a.	Encryption of removable media	Mandatory			
16b.	Encryption of removable media	Recommended			

17.	Secure transfer	Recommended			
18.	Implement controlled disposal of records	Mandatory			
19.	Malware Protection	Mandatory			
20.	Regular encrypted backup	Recommended			

21.	Ensure Business Continuity	Mandatory			
22a.	Secure disposal	Mandatory			
22b.	Secure disposal	Recommended			
23.	Implement a ‘whistle-blowing’ procedure	Recommended			

	Requirement	**Mandatory / Desirable**	**Fully Compliant, Partial Compliant, Non-Compliant (please note where this is N/A)**	**Evidence**	**Actions to address partial or non-compliance**
24	Conduct independent penetration testing	Recommended			