



Legal Aid
Agency

Data Security Requirements

LAA Information Security – Oct 2025

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 |
|---------|------------------------------|------------------------------|-------------------------|
| 5.0 | 1 st October 2025 | 1 st October 2025 | LAA Corporate Assurance |

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 | 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. |
| Table of reference documents | | | All links/documents have been updated to quote the latest versions. |

| Table of reference documents (Oct 2021) | HM Government Security Policy Framework | Government Functional Standard GovS 007 - Security | |
|---|--|--|--|
| 1 | The Legal Services Commission (“ LSC ”, “ we ”, “ us ”) is registered as a Data Controller with the Information Commissioner’s Office, in accordance with section 18 of the Data Protection Act (DPA) 1998 [Ref. 2]. Its Notification reference is Z6467906. This Notification sets out the purposes for which the LSC processes personal data. | The Ministry of Justice (MoJ) is registered as a data controller with the Information Commissioner Office’s, in accordance with section 18 of the Data Protection Act (DPA). Ref [2] | The LAA is now an agency of the Ministry of Justice and as such the MoJ is registered as the Data Controller with the Information Commissioner’s Office. |
| 1 | This Notification sets out the purposes for which the LAA processes personal data. | The LAA publishes privacy notices setting out the purposes for which the LAA processes personal data | |
| 1 | to comply with the Principles | to comply with the Data Protection Principles set out in UK GDPR | Revisions to previous changes to be clear which principles were being referred to. |
| 1.1 (Oct 2025) | | [INSERTION] - 1.1 Effective Dates | Section added to ensure clarity on which versions of the requirements applied. |
| 2 | | [INSERTION] – Policies – Ref 12A | Updated to include the Government Security Classification System introduced in April 2014. |
| 2 (Sept 2024) | All requirements renumbered – See Annex 3 | | Successive previous amendments had resulted in confusing numbering. Old and new numbers are detailed in Annex 3 |
| 2 (Sept 2024) | | [INSERTION] Policies 05a - Notes Remote/Home Working Policy detailing security arrangements/procedures (where such working is permitted by the Contract). | Additional requirement to maintain a Remote or Home Working policy where such working practices are permitted by the Contract. |
| 2 (Sept 2024) | Privacy Impact Assessment | Data Protection Impact Assessment | Amendment to Requirement 10 from PIA to DPIA. |

| | | | |
|---------------------|--|--|---|
| 2 (Sept 2024) | | [INSERTION] 19 – Recommended requirement to hold Cyber Essentials Plus certification. | Additional recommended requirement in line with government procurement policy and government security standards. |
| 2 | | [INSERTION] Testing and Assessment - Req. 20- Conduct independent penetration testing – Recommended. | Independent penetration testing of systems that store process or transmit information relating to 100,000 or more identifiable individuals. |
| 2 (Sept 2024) | Requirement 17 - 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 5 years | Requirement 17 - 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 | Reduced recommended review period from 5 years to 3 years. Pace of technological change and innovation and increased cyber security risk justify shorter review period for system risk assessments. |
| 2 (Oct 2025) | | [INSERTION] – Requirement 19a To hold Cyber Essentials certification for the life of the contract, or an equivalent standard. | New mandatory requirement to hold Cyber Essentials |
| 2 (Oct 2025) | Requirement 19 | Requirement 19b [INSERTION] or an equivalent standard. | Existing recommended requirement 19 renamed as 19b and additional line on equivalent standard is added. |
| 2 (Oct 2025) | Requirements 20, 22-28 | [REMOVAL] Requirements 20 22-28 | Technical requirements previously set out as 22-28 are now replaced by 19a, requirement for Cyber Essentials. Existing requirement 21 is renumbered to 20 |
| Annex 1 | | Annex 1 | This Annex has been added to reflect the requirements of Article 28 of UK GDPR. |
| Annex 2 | | Annex 2 | This Annex has been added to reflect the requirements of Article 28 of UK GDPR. |
| Annex 3 (Sept 2024) | | Annex 3 | This Annex has been added to detail the renumbering exercise of organisational and technical requirements. |

Provider Data Security Requirements

| | | | |
|-----------------------|--|---------|--|
| Annex 3 (Oct 2025) | | Annex 3 | Annex updated to match amendments to requirements 19, 20, 22-28. |
|-----------------------|--|---------|--|

Contents

| | |
|--|-----------|
| Version Control | 1 |
| Version History | 1 |
| Referenced Documents | 6 |
| 1. Data Security Requirements | 7 |
| 2. Requirements | 9 |
| Annex 1 – Processing of LAA Data | 12 |
| Subject Matter of the Processing | 12 |
| Duration of the Processing | 12 |
| Nature and purposes of the processing | 12 |
| Type of Personal Data | 12 |
| Categories of Data Subject | 12 |
| Return and Destruction | 12 |
| Annex 2 – Processing of Shared Data | 13 |
| Subject Matter of the Processing | 13 |
| Duration of the Processing | 13 |
| Nature and Purposes of the Processing | 13 |
| Type of Personal Data | 13 |
| Categories of Data Subject | 13 |
| Return and Destruction | 14 |
| Annex 3 – Renumbering of Requirements | 15 |

Referenced Documents

The following is a list of documents with a direct bearing on the contents of these requirements. 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 Guidance | v.5 October 2025 | Legal Aid Agency |
| 2 | Data Protection Act | 2018 | HMSO |
| 3 | Government Functional Standard GovS 007 – Security | July 2020 | Cabinet Office |
| 4 | ISO 27001 | 2022 | 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 |

1. Data Security Requirements

The Ministry of Justice (MoJ) is registered as a Data Controller with the Information Commissioner's Office, in accordance with the Data Protection Act 2018 (DPA) [Ref. 2].

The Legal Aid Agency ("LAA", "we", "us") is responsible to the MoJ for ensuring data is kept secure. The LAA publishes privacy notices setting out the purposes for which the LAA processes personal data [Ref. 6].

The LAA must receive assurances from you as one of its Providers¹ that you have taken every reasonable and appropriate measure to maintain the security of the data you will be processing on its behalf or shall be processing in common with the LAA. In order to achieve that objective, the LAA has prepared this document which sets out the basic security requirements that need to be followed, and a separate more detailed document titled Data Security Guidance [Ref. 1] which provides further information on how these requirements must be met.

In the LAA, the processing and sharing of personal data is governed by the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR).

The LAA requires its Providers and any third parties appointed by Providers in accordance with the LAA contract to comply with the Data Protection Principles set out in UK GDPR to ensure that LAA can fulfil its obligations under the Data Protection and Freedom of Information Acts.

In addition, as an Agency of the MoJ, the LAA is required to comply with Government Functional Standards, specifically Standard 007 – Security [Ref. 3].

These requirements may change in future as Government policies change to accommodate lessons and new developments. You must work co-operatively with us to ensure that any new obligations are complied with in accordance with the LAA Contract.

For the avoidance of doubt, where you are a Provider to the LAA you are required to have regard to the LAA Data Security Requirements i.e. this document.

The nature of the services provided by the LAA means that clients will entrust the LAA with their personal data, which may include sensitive personal data. The LAA has an Information Charter [Ref. 7], which provides assurance to clients that we will keep their data secure at all times.

We require LAA Providers and any third parties appointed by Providers in accordance with the LAA contract to have secure organisational and technical measures in place to protect

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

the personal data from unauthorised or unlawful processing, accidental loss, destruction or damage and to maintain the confidentiality, integrity and availability of information.

Instructions regarding the processing of LAA Data² is set out at Annex 1 of this document and instructions regarding the processing of Shared Data is set out at Annex 2 of this document. Annex 2 also sets out a description of the joint controller relationship in respect of Shared Data.

You shall comply with any further written instructions of the LAA with respect to processing.

1.1 – Effective Dates

Version 3 of the Data Security Requirements and Guidance apply to all contracts coming into force before 1st September 2024

Version 4 of the Data Security Requirements and Guidance apply to all contracts coming into force on or after 1st September 2024 and before 1st October 2025

Version 5 of the Data Security Requirements and Guidance apply to all contracts coming into force on or after 1st October 2025.

² LAA Data and Shared Data are defined by the Contract Standard Terms and that definition is applied to this document.

2. Requirements

The following table shows the organisational and technical measures that Providers should have in place. The Req No column is used to cross reference to the Data Security Guidance [Ref. 1] that sets out further details on how these requirements should be met.

| Area | Req No. | Requirement | Mandatory or Recommended | Notes |
|------------|---------|---|--------------------------|--|
| Governance | 01 | Register as a Data Controller | Mandatory | To be registered as a Data Controller with the Information Commissioner's Office unless an exemption applies. |
| Governance | 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. |
| Culture | 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. |
| Culture | 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. |
| Policies | 05a | Have a coherent set of policies | Mandatory | Must have policies covering: <ul style="list-style-type: none"> • 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). |
| Policies | 05b | Have a coherent set of policies | Recommended | Should have policies covering: <ul style="list-style-type: none"> • Clear Desk Policy |

| | | | | |
|------------|----|---|-------------|--|
| | | | | <ul style="list-style-type: none"> 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. |
| Policies | 06 | Undertake an annual review | Mandatory | To have in place procedures to review all data protection and information security policies at least annually. |
| Policies | 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. |
| Compliance | 08 | Monitor and Report | Recommended | Monitor compliance with data protection and security policies and produce an annual audit report. |
| Procedures | 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. |
| Procedures | 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. |
| Procedures | 11 | Conduct staff screening | Mandatory | Conduct appropriate screening of staff and carry out background checks to ensure reliability. |
| Procedures | 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. |
| Procedures | 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. |
| Procedures | 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. |
| Disposal | 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. |
| Disposal | 16a | Secure disposal | Mandatory | Dispose of electronic media holding LAA Data or Shared Data through secure destruction |
| Disposal | 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 (T8a) upon permanent disposal. |
| Risk Assessment | 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 |
| Risk Assessment | 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. |
| Standards | 19a | Cyber Essentials | Mandatory | To hold Cyber Essentials certification for the life of the contract, or an equivalent standard. |
| Standards | 19b | Cyber Essentials Plus | Recommended | To hold Cyber Essentials Plus certification and renew / maintain as required, or an equivalent standard. |
| Compliance | 20 | Ensure Business Continuity | Mandatory | Create and implement business continuity plans. Create and implement disaster recovery plans. |

Annex 1 – Processing of LAA Data

Subject Matter of the Processing

For the LAA's purpose, to allow the LAA (and where appropriate delegated to providers) to make decisions about the grant of funding including the eligibility of the client, to monitor the progress of the matter, to make any further decisions as to case management or additional funding for the case, to make payments in respect of work done and to manage any financial contributions paid by the client or the operation of the statutory charge.

Duration of the Processing

For the duration of the contract and if the case progresses beyond the contract term then for the duration of the case.

The duration of the case may include processing in respect of outstanding debts owed to the LAA.

Nature and purposes of the processing

Processing by means of collection, recording, use and disclosure between parties. You process the LAA Data as part of the LAA's statutory function that is delegated to you in order to provide legal services to LAA funded clients.

Type of Personal Data

Name, address, date of birth, ethnicity, disability information, details of family members (where required), financial information (where required), facts of the case, data relating to criminal convictions (where required), medical and expert reports (where required) and other Special Category data (where relevant to the proceedings).

Categories of Data Subject

Clients and other parties involved in the proceedings, including where relevant respondents, experts, victims, witnesses and family members of the client.

Return and Destruction

Data must be returned to the LAA or destroyed once the processing is complete unless a requirement in law is identified to preserve that type of data.

The LAA retains data in accordance with its Records Retention and Disposition Schedule.

<https://www.gov.uk/government/publications/record-retention-and-disposition-schedules>

Data will not be retained for longer than is necessary in line with the retention schedule and the contract.

Annex 2 – Processing of Shared Data

The LAA and you are joint controllers of the Shared Data and the relationship reflects a “controllers in common” relationship as the LAA and you are both controllers of the same data, although the LAA and you sometimes process it for different purposes and independently of one another.

A description of the processing undertaken in respect of the Shared Data is set out below.

Subject Matter of the Processing

For the LAA’s purpose, to allow the LAA (and where appropriate delegated to providers) to make decisions about the grant of funding including the eligibility of the client, to monitor the progress of the matter, to make any further decisions as to case management or additional funding for case, to make payments in respect of work done, to manage financial contributions paid by the client or the operation of the statutory charge and to audit any of the above where such tasks have been delegated to providers.

Duration of the Processing

For the duration of the contract and if the case progresses beyond the contract term then for duration of the case.

The duration of the case may include processing in respect of outstanding debts owed to the LAA.

Nature and Purposes of the Processing

Processing by means of collection, recording, use and disclosure between the parties. Both parties process the Shared Data for their own purposes.

You need to collect the Shared Data to enable you to act for your client.

The LAA processes the Shared Data to monitor the progress of the matter, monitor the funding of the matter and where relevant, audit the processing of LAA functions that have been delegated to you.

Type of Personal Data

Name, address, date of birth, ethnicity, disability information, details of family members (where required), financial information (where required), facts of the case, data relating to criminal convictions (where required), medical and expert reports (where required) and other Special Category data (where relevant to the proceedings).

Categories of Data Subject

Clients and other parties involved in the proceedings, including where relevant respondents, experts, victims, witnesses and family members of the client.

Return and Destruction

You should document your own retention periods and destruction processes for Shared Data held by you to meet the requirements of the contract and other obligations for retention of data that may be set out by statute, or professional bodies.

The LAA retains data in accordance with its Records Retention and Disposition Schedule.

<https://www.gov.uk/government/publications/record-retention-and-disposition-schedules>

Data will not be retained for longer than is necessary in line with the retention schedule and the contract.

Annex 3 – Renumbering of Requirements

The following table shows the numbering of each requirement as set out in this version of the Requirements and as set out in Version 3

| Area | Req No. | Requirement | Version 3 No. |
|-----------------|---------|---|---------------|
| Governance | 01 | Register as a Data Controller | 3 |
| Governance | 02 | Appoint a Data Protection Supervisor | 4 |
| Culture | 03 | Foster a culture that values and protects information | 1 |
| Culture | 04 | Maintain a level of staff awareness | 6 |
| Policies | 05a | Have a coherent set of policies | 12a |
| Policies | 05b | Have a coherent set of policies | 12b |
| Policies | 06 | Undertake an annual review | 12c |
| Policies | 07 | Have in place an Incident Management Policy | 13 |
| Compliance | 08 | Monitor and Report | 8 |
| Procedures | 09 | Implement a 'whistle-blowing' procedure | 23 |
| Procedures | 10 | Conduct Data Protection Impact Assessments | 11 |
| Procedures | 11 | Conduct staff screening | 5 |
| Procedures | 12 | Control access to personal data | 2 |
| Procedures | 13 | Maintain access records | 7 |
| Procedures | 14 | Maintain adequate physical security | 14 |
| Disposal | 15 | Implement controlled disposal of records | 18 |
| Disposal | 16a | Secure disposal | 22a |
| Disposal | 16b | Secure disposal | 22b |
| Risk Assessment | 17 | Conduct formal, documented risk assessments. | 9 |
| Risk Assessment | 18 | Apply appropriate controls | 10 |
| Standards | 19a | Cyber Essentials | New |
| Standards | 19b | Cyber Essentials Plus | New |
| Compliance | 20 | Ensure Business Continuity | 21 |
| Removed | | Hard disk encryption | 15a |
| Removed | | Hard disk encryption | 15b |
| Removed | | Encryption of removable media | 16a |

Provider Data Security Requirements

| | | | |
|---------|--|-------------------------------|-----|
| Removed | | Encryption of removable media | 16b |
| Removed | | Regular encrypted backup | 20 |
| Removed | | Secure transfer | 17 |
| Removed | | Malware protection | 19 |