

G-Cloud 15: Service definition

Link Maker Systems Ltd

Children's Social Care Placement Platform

Lot 2b Software as a Service (SAAS)

Link Maker Systems

support@linkmaker.co.uk

www.linkmaker.co.uk

0800 368 8549



Contents

Link Maker Systems Ltd.....	1
Contents.....	2
1. Introduction.....	3
2. Data Protection.....	7
Data in transit protection	7
Asset Protection and resilience	8
Separation between consumers	9
Governance framework	10
Operational security	10
Personnel security	11
Secure development.....	12
Supply chain security	13
Secure User Management.....	14
Identity and Authentication	15
External interface protection.....	15
Secure service administration	16
Audit information and alerting for customers.....	17
Secure use of the service.....	17
3. Social value statement	19
4. Using the service	20
5. Provision of the service	24
6. Our experience	25
7. Clients	29
8. Contact details	30

1. Introduction

Company Overview

Link Maker Systems (LMS) is a social enterprise founded by two people with personal experience of children's social care. Realising how much children's social care could benefit from being more joined-up, today, our full-time development and support staff provide an online platform across the UK, spanning adoption, fostering & children's homes, and commissioning.

Our vision is for all looked after children to find stable relationships with those who can best meet their individual needs, and to receive the right support to help them recover from past experiences and flourish. We believe information is key, and aim to:

- Give access to the widest range of placements to improve needs-led decisions for children
- Improve knowledge of national sufficiency to inform recruitment and development of new provision
- Help to build a national picture of children's journeys and wellbeing, to show that early investment brings rewards for everyone.

We develop our platform using an 'agile' process, which involves frequent updates in response to changing needs. This is informed by an exchange of experience and ideas within an advisory group of experts and national leads.

Link Maker is used by all of the Local Authorities in England and is used for the National Adoption Register for Scotland and Wales.

Value Proposition

Independent reviews of residential and foster care in 2016 and 2017 highlighted a wide range of problems in the placement commissioning process, and in both cases the use of Link Maker was recommended. The problems included a poor understanding of sufficiency, poor knowledge of available placements, poor matching, lack of vacancy management, inefficient and ineffective referral processes, poor involvement of foster carers, too little attention to children's wishes, and lack of peer-support for foster carers.

Within adoption, Link Maker proactively met the need for a faster, more efficient way of exchanging information when seeking placements, and for family-finders to have instant knowledge of available adopters, and the right tools to find the most suitable family for a specific child. Due to the rapid take-up of the platform across the UK, a uniquely detailed and up-to-date picture of children's needs and adopter's capabilities became available for the first time.

Overview of the G-Cloud Service

For Adoption

Link Maker increases placement choice for children awaiting adoption, creating a UK-wide pool of available adopters, and improving the use of data and collaboration between local authorities and independent adoption agencies. Over 4,600 children have been matched since the platform was launched in 2014.

Local authorities' family-find for children by approaching suitable adopters, or by listing the child's profile if appropriate. Link Maker's support team works proactively to ensure no child 'falls through the cracks'. Progress is closely monitored, and where it appears more could be done for a child additional advice and support is offered to their social workers.

How does Link Maker help children's services?

- Forming Regional Adoption Agencies. A comprehensive range of collaboration features for regional services and consortia are available including bespoke branding.
- Access the widest range of families. The detail contained in profiles guides family-finders to families who may best meet a child's needs, whether in-house, from a RAA or provider group, or nationally.
- Show interest in families from your region or across the whole of the UK. Available family profiles can be searched, filtered and ordered according to a range of geographical and other criteria, and approaches made to invite discussions.
- Invite interest from families. Issue child profiles to in-house families, or to external families according to geography, consortia, and other criteria.
- Schedule profile visibility. According to the policy in each case, the visibility of child profiles can be automatically increased from, for example, in-house, to a small geographical area, to a larger area, at appropriate intervals. The sequence can be set to stop automatically when enough interest has been shown.
- Involve and support families. Social workers can share details with their families and empower them to help identify suitable matches where appropriate. Families can be supported online by appropriate staff during family-finding and post-placement.
- Meet data protection obligations. All documents and messages are shared securely with local authorities and families, with information encrypted using the password of the intended recipient, and made available to them for only as long as it is needed
- Motivate families to search themselves. Adopters can self-register, be verified by the agency and Link Maker support and then identify matches themselves, with the support of their workers.
- Family-find in both Welsh and English. The system is fully translated into both languages and has features to enable the timely, and inline, translation of profiles by agencies into both languages.

- Keep information up to date. All users can update their profiles and cases directly, in real time. Link maker monitors all cases for inactivity, and our support team works directly with users to make sure all information is up to date.
- Manage cases flexibly. All users accounts are specific to individuals, so that cases can be shared between managers and social workers according to prevailing practice and policy in the organisation.
- Child-level reports. Instant reports can be run containing evidence of available families, and of family-finding activity conducted on behalf of a child or sibling group.
- Effective oversight. A range of user-level permissions can be applied, granting the ability to view activity against all cases and to run detailed activity reports.
- Plan ahead. Live data is always available and can be aggregated regionally and nationally. Powerful reports and dashboards enable supply and demand to be monitored effectively, in real time.
- Online presence. Manage a customised, branded portal for staff and families from your organisation. This can bring together both family-finding and support, and can provide news and information, advertise, and facilitate events, hold forums for practice discussion and peer support, and make family-finding profiles available to appropriate users.
- The website is partially compliant with the Web Content Accessibility Guidelines version 2.1 AA standard, please see [Accessibility here](#) Ongoing development. Nothing in children's social care stands still, and Link Maker's continuous development is shaped by feedback and suggestions from users.

Placement commissioning

In November 2016 Link Maker launched a commissioning platform. Link Maker can help local authorities and placement providers to improve process, collaboration, and intelligence, as recommended by major reviews of the sector.

Recent reviews of both fostering and residential care have recommended that the advances brought to adoption by Link Maker be explored in other care settings. Link Maker's commissioning platform is available to local authorities and placement providers interested in changing the way they work

How could the platform help you?

- Considering all vacancies according to a child's individual needs, with in-house and all external providers in one place, and subsequently filtering for cost and other considerations.
- Providers listing live vacancies for placement officers to review, increasing the chance of suitable placements being found quickly, and building a picture of sufficiency
- Involving more of the team around the child, and children themselves, in reviewing placement options.
- Collaboration between authorities to pool in-house foster carers, improving matching and use of resources.
- Greater control for providers in determining the nature of referrals they receive, and from which authorities.

2. Data Protection

Data in transit protection

Network Security Management

LMS Infrastructure, including security configurations, of hardware, software, services, and networks is documented, implemented, monitored, and reviewed to safeguard the integrity, confidentiality and availability of the platform.

Changes to the LMS Infrastructure are approved by the Technical Architect and managed through the LMS Infrastructure Change Process.

LMS will protect the infrastructure using defence in depth principles, creating multiple layers of security controls to protect the network from diverse attack vectors

Network security is supported by [Access control policy](#), [Threat intelligence](#), and [Communications Security](#).

Communications security

Security in Information Transfer

LMS Customers can access web services through HTTPS and using a combination of username, password, and PIN. In addition to TLS, LMS use CSRF and XSS protection.

There is a list of supported file types that can be uploaded from users to the internet facing applications that LMS manage. Permitted file types are managed by the application. All files are virus checked and meta data is stripped from the file on upload before being stored on the LMS infrastructure.

End users of the service must agree to the terms and conditions of the LMS online services which include provisions on security. Furthermore, a security page is hosted on all LMS web servers detailing security controls and contact information for any security concerns

Cryptography

LMS defines that application data must be protected in transit and at rest, using strong cryptographic algorithms in line with industry standard guidelines, that provide effective protection against unauthorised access and theft of data.

Cryptographic keys are generated, stored, and managed in a secure manner that prevents loss, theft, or compromise.

Access to cryptographic keys is restricted to authorised individuals.

LMS use AWS Key Management Service (KMS). AWS Key Management Service (KMS) provides centralized control over the cryptographic keys used to protect LMS data. AWS KMS is

designed so that no one, including AWS employees, can retrieve plaintext keys from the service. Access to AWS KMS is controlled by AWS IAM.

All AWS services (RDS, EFS and EC2) are encrypted at rest using keys managed with the AWS Key Management Service (KMS).

For data classified as '**highly sensitive**' the LMS application uses a combination public key (asymmetric) and symmetric cryptography methods to secure the data; everyone's access to content is secured using a unique key to that user, derived from a combination of data provided during their log in which is only available to that user in their session.

Each organisation and family users of the web applications has an associated public/private key pair which is used to encrypt sensitive data; practitioners of an organisation have access to data via their organisation's key.

Admin users have access to keys for administrative purposes and restoring lost access to users but do not have application-level access using these to view content.

Access to SSH services on the EC2 instances is restricted to source locations from within the VPC or on the Client VPN which terminates with the VPC. Authentication are restricted to public key authentication mechanisms.

Asset Protection and resilience

Physical/Environmental security for LMS platform

The online services which are provided by LMS to its customers is hosted in locations which have advanced physical security control measures in place, for example data centre security controls including access control, CCTV and 24-hour monitoring.

Data centre locations are chosen to mitigate environmental risk, such as flooding, extreme weather, and seismic activity. The data centres are climate controlled, with automatic detection of water or fire and suppression equipment and power redundancy

The virtual hosting environment is spread across two availability zones and can be switched from one to another within in minutes, therefore there is no single point of failure with regards to geographic sites.

LMS AWS data centres are in the UK, and has certification for compliance with ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015, and CSA STAR CCM v4.0.

The current uptime for AWS is 99.99%.

Backups

Backups of the application servers and database server managed by AWS Backup which allows automated scheduled backups, retention management and activity monitoring for audit purposes. The EFS and RDS servers on production are backed up nightly and kept for

2 weeks, weekly backups for 8 weeks, monthly backups for 12 months and a yearly backup for a year.

Backups are encrypted at rest and in transit and stored in a dedicated backup vault.

Backups are tested during monthly DR tests.

Data encryption

Please also see [Communications security](#)

Data sanitisation/deletion

We only retain information regarding placements for as long as it is relevant. Removal of data can be instigated by:

- The user
 - o Case data is held on the system for a period of 20 days
 - o When marked for deletion after 20 days all data is anonymised, and information is held for statistical purposes only
- LMS carry out regular checks for records considered to be idle (inactive), and as a support task will contact the user to ensure that the records are still accurate and required and take appropriate action.
 - o Case data is held on the system for a period of 20 days
 - o When marked for deletion after 20 days all data is anonymised, and information is held for statistical purposes only

Electronic database records are deleted at the request of the users or in accordance with the LMS Record Retention Schedule, which details the record types and procedures for deletion. This is detailed for users in the LMS Privacy Policy.

Deletion date, reason and user id of the person or system process is recorded in against the data base record

Data records are marked for deletion, and the data is anonymised in accordance with the 'Anonymisation Code of Practice' issued by the ICO and any encryption keys deleted. This anonymised data is held by LMS for statistical purposes.

Separation between consumers

The Link Maker platform can be accessed by all local authorities, voluntary adoption agencies, independent foster care providers, and residential homes. This is a data exchange service, and information can be shared across the platform but only at the request of the user.

Governance framework

The LMS ISMS sets out LMS commitment to security, its information and services. It applies to all personnel, assets, internal and external services, and any information stored.

LMS are Certified to ISO270001- <https://www.linkmaker.co.uk/doc/ISO27001.pdf>

Operational security

Threat Intelligence

LMS recognises the importance of threat intelligence, to prevent, detect and respond to threats.

LMS engage a threat detection service that continuously monitors our instances servers, user access, databases, and storage for potential threats. Using anomaly detection, ML and behavioural modelling and threat intelligence feeds from AWS and leading third parties (AWS Guard Duty).

AWS Security Hub integrates with Guard Duty to aggregate its findings. Security Hub offers a centralized view, combining Guard Duty's real-time threat detection for comprehensive security monitoring.

Our hosting provider is alerted to any possible threats and LMS employ Cloud Native Security, where Rackspace security specialists will monitor and analyse the above and act according to a specified runbook.

A Rackspace ticket will automatically be generated to notify LMS administrators of any potential threats and recommended mitigations for lessons learned as part of continual improvement.

Technical Vulnerability Management

LMS utilise AWS Security Hub which monitors for vulnerabilities, and measure against AWS Security Best Practices V 1.0.0 and AWS CIS benchmarks v1.2.0. The AWS Security Hub is reviewed by the Security officer on a regular basis. LMS also use a vulnerability scanner that identifies software flaws, misconfigurations, and security weaknesses, this is run daily on our EC2 templates, if any vulnerabilities are detected It is flagged to the security officer and automatically updated/patched.

Management of Information Security Incidents & Improvements

LMS have a dedicated security incident policy, process, and log template. These must be read and understood by all LMS staff and contractor(s). It is everyone's responsibility to report suspicious or confirmed security incidents to the LMS security officer.

Configuration and change management

Configuration management, including security configurations, of hardware, software, services, and networks is documented, implemented, monitored, and reviewed.

Any changes to configuration of the LMS platform architecture is approved by the Technical Architect and reviewed against impact on the LMS security policies before being approved and managed through the LMS Infrastructure Change Process.

The configuration of the LMS infrastructure is reviewed periodically and updated in response to new threats of vulnerabilities, new software versions or in response to performance or capacity issues.

LMS use AWS AMI, which is a custom pre-configured template that contains the necessary files, operating system, and software configurations to launch EC2 images.

Hardware and software configuration is documented, and any changes to the AMI image are tracked through the LMS Infrastructure Change Process.

Access to AMI templates is restricted to administrator users on the systems.

LMS uses an automated script, to deploy specified versions of code to update the AWS infrastructure.

Personnel security

LMS Employees

All personnel who work for LMS must have background checks applied to ensure they do not introduce an unacceptable risk to the organisation. Checks will include prior employment and identity checks. All staff must have CRB/Disclosure Barring Service checks carried out before gaining employment with LMS. And DBS checks are renewed every two years.

Staff employment contracts include terms and conditions that relate to the security of LMS assets and staff adhering to LMS policies and procedures, and confidentiality clauses.

Bi-annual security training is provided to all staff.

Access control policy

LMS have implemented a high-level policy for its organisation.

Access control underpins all security as it enables information and systems to only be seen and accessed by those with proper authorisation. Poor access control policies enable unauthorised individuals to see or modify access to information and systems causing a severe impact on LMS business and service offerings.

System and Application Access Control

LMS admin users can only access the application from a specified IP address. It is not possible to access the web site application over HTTP, and all insecure HTTP requests are redirected to HTTPS.

Access to the LMS application source code should be limited to the site developers and security officer only.

Within the LMS platform access to privileged utility programs (for example command shells) must be limited to the hosting provider, system administrator/developers.

Secure development

Security requirements for engineering

LMS are committed to ensuring their services remain secure. LMS Security requirements for engineering captures security requirements for the development of the solution including the infrastructure.

Implementing security requirements for engineering can significantly reduce the risk of security breaches and protect both the organization and its stakeholders from potential harm. It's important to involve all relevant stakeholders, including developers, security professionals, and management, in the development and enforcement of the policy.

The requirement policy will be reviewed annually, and in response to security incidents raised, adapt to changes in technology, emerging threats, and newly discovered vulnerabilities. Continuous improvement and adaptation are key to maintaining the effectiveness of the policy over time.

We will not define the full policy here, but it covers Secure coding, Application security and Hosting provider security requirements.

Development environments

The virtual infrastructure resides at AWS and are managed by Rackspace. The production instance is across multiple availability zones, the non-production (test) instance is on a single availability zone.

The staging and live environments are both on the production instance, so that prior to deployment we are testing in an environment as close to the live environment as possible.

See also [Configuration and Change management](#)

Deployment procedure

Following approval from Director of Operations, Technical Architect or more senior, authorised personnel use an AMI deployment scripts to deploy the version of code specified. This will pull from a private GIT repository showing only tagged releases.

LMS use a Blue/Green deployment strategy,

Supply chain security

Information Security in Supplier Relationships

LMS mandates that suppliers including those of cloud services, processing personal data from the LMS platform meet LMS' own internal standards and regulatory requirements about Information security. They must demonstrate that they are able to maintain the confidentiality, integrity and availability of the data at all times.

The requirements laid down in "LMS Security Requirements for Engineering" in Section 4 apply to third parties who host services on which LMS depend.

Prior to procuring services suppliers will be evaluated and any risk assessments conducted by the security officer to ensure they meet appropriate security standards and signed off by the CEO.

Initially a high-level review is completed of the supplier and any of their sub-processors to establish the types of data that is processed, their compliance with applicable data protection legislation and to ensure that they have sufficient guarantees to implement appropriate technical and organisational measures to meet requirements of GDPR and protect the rights of the individual data subjects. A DPIA is conducted where necessary see [M].

A secondary more detailed review is then conducted. LMS review the reputation and reliability, service levels and an appointment and exit plans. In addition, there is a review of the supplier's information security and data protection related policies and procedures to ensure that they meet LMS' own internal standards and regulatory requirements. In particular policies relating to Business continuity, HR security & training, and Physical and technical measures taken to protect the LMS data. For cloud suppliers we ensure that they meet the [UK government's Cloud Security Principles](#).

Supply chain

Evaluation, and review of any suppliers also includes that of any sub-contractors and processors of the data, or components of the services provided. All suppliers must ensure that the required security standards are adhered to throughout the supply chain. Any changes to the supply chain must be communicated with LMS.

Supplier Agreements

Supplier agreements should be established to ensure that there is clear understanding between LMS and the supplier regarding both parties' obligations to fulfil data protection, access controls, incident reporting and compliance with the relevant security standards and regulations.

Supplier Service Delivery Management

LMS require that suppliers are regularly monitored, reviewed, evaluated and any change managed in the supplier relationship to maintain the agreed level of information security and service delivery. Including any ongoing improvement initiatives to address any identified security gaps.

Secure User Management

Verification of users

Users of LMS systems for family-finding cannot access content until their identity has been checked and they are authorised by a Local authority or voluntary adoption agency. This is usually carried out by requesting information from the user's nominated authority. Or by an organisation 'verifier' (see below)

User roles

Organisation default user

A default role exists for practitioners of an organisation on Link Maker allowing them to do the following.

- View child profiles
- Create child profiles
- View adopter profiles
- Create adopter profiles
- Manage profile availability

These permissions are standard for managing the family finding process. However, manager or verifiers within an organisation can restrict an individual's access. This can be achieved from the main navigation bar, select admin, verify users, or main navigation bar, select admin, manage accounts

Manager user

Management and verification permissions for an organisation can be applied to an organisation's user. These permissions are only applied on request from an organisation's management and applied by LMS administrators.

- **Verification** - ability to verify users within an organisation and apply user permissions regarding creation and visibility of profiles and involvement in discussions. This can be achieved from the main navigation bar, select admin, verify users
- **Management** - Management permissions are separated
 - o Access to data exports, these can be accessed from his can be achieved from the main navigation bar, select admin, organisational reports, data exports.
 - o Access to verify user accounts, disable and manage permissions of practitioner accounts. This can be achieved from the main navigation bar, select admin, manage accounts

Identity and Authentication

Authentication of users

All accounts will be required to use Multi-Factor Authentication (MFA) to access the system. When logging in, the practitioner will have to provide a username, strong password (12 characters both alpha and numeric) and three digits from a PIN. If the device does not include a unique encrypted cookie (familiar device) for that user a onetime code will be emailed to the user's verified email address or sent to their confirmed mobile phone number by SMS. This will then need to be entered online to complete the login process.

Users input their credentials, and on successful validation of these credentials, a cookie is saved to the user's browser identifying their session data on the server. This cookie, and the associated session data, is checked on every page request, and the user's role is ascertained.

In the event of a password being forgotten by a user they are provided with options to reset it on the login page. On request, a link to reset the password is sent to the users email account. Users are not permitted to reuse a password that historically has been used by the system.

Those users with 'Manager permissions' can manage users permissions.

External interface protection

Robust cybersecurity

Protecting ICT systems from cyber threats is a fundamental aspect of business continuity. Employing robust cybersecurity measures, [Network Security](#), [Anti-malware](#), [Cryptography](#), and [regular security audits](#), can help safeguard critical data and systems from unauthorized access or cyber-attacks.

See also [Security Requirements for Engineering](#)

Protection from Malware

All devices which support both corporate and LMS services use Anti-malware software which is updated automatically (for data centre hosted items).

Technical Vulnerability Management

LMS utilise AWS Security Hub which monitors for vulnerabilities, and measure against AWS Security Best Practices V 1.0.0 and AWS CIS benchmarks v1.2.0. The AWS Security Hub is reviewed by the Security officer on a regular basis.

Logging and Monitoring

The servers, services and application generate logging information for all user (both end user and privileged user) actions within the application. These are stored on AWS Cloud Watch, in the datacentre.

All logs are protected from access by unauthorised individuals. Access to logs is monitored and only administrator users on the systems can access logging information.

The servers and services are monitored both by Rackspace and LMS, alerts are triggered by key metrics relating to CPU, Memory, data traffic. In the event of an alert, it will be reviewed by either the security officer or responsible administrator.

In addition, LMS employ Cloud Native Security, where Rackspace security specialists will monitor the following for critical issues, and act according to a specified runbook. AWS Guard Duty, a threat detection service that continuously monitors for malicious or unauthorised behaviour. IAM Access Analyser, which enables LMS to verify that their policies provide exactly the level of access required. It continuously monitors for new or updated policies, and analyses permissions granted using policies for Amazon S3 buckets, AWS KMS keys, Amazon SQS queues and AWS IAM roles. All data is pulled together in the AWS Security Hub, which also provides compliance standard checks against industry best practice (e.g., CIS AWS foundations).

Secure service administration

LMS conduct risk assessment to identify potential threats to ICT systems, This involves evaluating vulnerabilities, such as hardware and software failures, cyber-attacks, natural

disasters, and human error, among others. By understanding these risks, LMS can better prepared to mitigate their impact on operations.

LMS completes the risk assessment annually, or in the event of a security incident, and will update business continuity plans accordingly.

Independent Review of Information Security

Link Maker Systems uses an external CESG-approved CHECK company to perform IT Security health checks to perform both network and application-level vulnerability tests. The findings are interpreted into a remediation plan which contains vulnerabilities which require fixing. This is maintained by the security officer and reviewed on a regular basis.

IT Health Checks are carried out at least annually or when a major software update/site is issued.

See also [Logging and Monitoring](#)

Audit information and alerting for customers

See also [Logging and Monitoring](#)

Logging and monitoring are an internal process for LMS and information is not routinely shared with customers.

LMS have 'LMS Data protection Policy and procedures', which sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection, handling, and storage of personal data. This includes how users can exercise their rights in terms of data protection, which is detailed for users in https://www.linkmaker.co.uk/pages/privacy_policy.

In the event of a data breach the LMS Security Officer to notify all parties involved If harm is likely to be caused to those persons whose information has been accessed, via email if breach is identified, and for those customers with specific contracts the DPO where listed.

Secure use of the service.

Privacy by Design

The LMS data protection policy sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection, handling, and storage of personal data, and to comply with GDPR and DPA.

The security officer ensures that the company board are updated about data protection responsibilities, reviewing all data protection policies and related procedures, checking, and approving and contracts and agreements with third parties that may handle the company's personal data and ensuring that LMS staff are given regular training to ensure they understand their responsibilities when handling data.

The company has a privacy statement, setting out how data relating to individuals is used by the company, and how users can exercise their rights.

Electronic database records are retained and deleted in accordance with the LMS Record Retention Schedule. The ICO requires that information is kept no longer than is required to fulfil its purpose. LMS carry out regular checks for records considered to be idle (inactive), and as a support task will contact the user to ensure that the records are still accurate and required and take appropriate action. There are instances when records are automatically deleted but only when the user has been given sufficient notification. These checks also apply to user records so permission to access sensitive data is only granted to appropriate individuals.

In addition to the infrastructure redundancy listed in the sections above, data is encrypted both in transit and at rest.

LMS carry out DPIA assessments in line with the guidance issued by the ICO – Conducting privacy impact assessments code of practice. During the design stage assessment questions are addressed and where it is deemed that a DPIA is required then the issue is escalated to the security officer as part of the software development process.

3. Social value statement

Link Maker Systems Ltd delivers digital solutions that support adoption and fostering services across the UK, directly contributing to social care outcomes covered by the Light Touch Regime.

Link Maker has always found ways to help strengthen communities of support for adopters and carers around the UK. A part of the platform was developed specifically for this purpose and has always been provided to service users free of charge.

Our mission is for all looked after children to find stable relationships with those who can best meet their individual needs, and to receive the right support to help them recover from past experiences and flourish, aligning with government priorities.

Community Engagement

We engage with DfE, local authorities/RAA's, Adoption England, Scottish and Welsh governments, Voluntary adoption agencies, independent fostering providers, Adopters and Birth family members to co-design services that meet the sectors needs and align with national guidelines.

Job Creation, Workforce Conditions and inclusivity

We are committed to creating and retaining jobs within the contract workforce while ensuring fair employment practices. All staff will have accurate employment contracts with clear review processes and pay will exceed the National Minimum/Living Wage, including statutory sick pay from day one. We monitor pay gaps and implement measures to tackle inequality in employment and progression opportunities.

Kinship carers will receive pay and leave equivalent to statutory adoption provisions. We also address barriers such as childcare and flexible working to promote inclusivity and workforce participation.

Skills Development & Progression

LMS have implemented measures to support in-work progression, offering training to help staff become more qualified. We work closely with staff to gauge workforce engagement and satisfaction, acting promptly on feedback to improve conditions.

Health & Wellbeing

LMS takes Health and safety issues seriously and is committed to protecting the health and safety of its staff.

Supply Chain

In addition to the security standards offered by potential suppliers LMS where possible will consider not only the social value they deliver in alignment with the Public Services (Social Value) Act 2012, but also their commitment to ethical standards and compliance with

modern slavery legislation, ensuring our procurement decisions promote integrity, fairness, and positive impact on the wider community.

Environmental impact

Our digital services reduce paper usage. LMS operate a remote working company, eliminating travel and supporting sustainability goals.

Measurement & Reporting

We will track and report on, jobs created and retained, training and progression metrics, and our community engagement activities.

4. Using the service

Ordering and Invoicing

Licences to cover an annual period can be purchased via invoice.

- The licence will be activated on receipt of a PO number or full payment of the invoice.
- Payment terms for invoice is 30 days.

Enquiries regarding a licence can be made to accounts@linkmaker.co.uk or by calling 0800 368 8549. Requirements regarding access levels and permissions for specific individuals, activation of user controlled licenced features or merging organisations can be agreed prior to licence activation.

Availability of Trial Service

An initial trial service is available on request, and on approval of an organisation's manager. This will allow access to the licenced features below for a month. During a trial the full features listed above for adoption and / or commissioning would be available to all staff within an organisation, covering:

- Comprehensive placement finding tools
- Secure communication and document exchange
- Involving and supporting families
- Dashboards and reporting features
- Collaboration with external organisations, or as part of a consortium

On-Boarding, Off-Boarding, Service Migration, Scope etc.

Users need to register on the site to create login information. Additional help/advice on creating profiles or managing family finding can be obtained from the support desk or video tutorials available online.

Two months prior to the licence expiry the organisation will be contacted regarding the renewal of the licence. If the organisation does not wish to renew the licence, then;

- Any reports or statistical information exports required will need to be run by the user prior to the licence expiry.
- Licenced features will no longer be available after the licence expiry
- Case data marked as inactive will be deleted after 3 months.

We only retain information regarding placements for as long as it is relevant. Removal of data can be instigated by:

A. The user

- Case data is held on the system for a period of 20 days
- When marked for deletion after 20 days all data is anonymised, and information is held for statistical purposes only

B. LMS carry out regular checks for records considered to be idle (inactive), and as a support task will contact the user to ensure that the records are still accurate and required and take appropriate action.

- Case data is held on the system for a period of 20 days
- When marked for deletion after 20 days all data is anonymised, and information is held for statistical purposes only

Training

The system is designed to be intuitive and make learning easy, however our support desk is available to answer any training issues.

We currently maintain a library of video tutorials which are available on the site, and provide a schedule of training sessions to licenced users.

We are also able to provide bespoke training days for organisations at a rate of £960 per day, as per the SFIA rate card.

Service Management

Planned site or infrastructure upgrades are schedule out of hours to minimise user impact, and advanced notice will be given of any service outage.

For any planned down time that exceeds 1 hour, users will be emailed 3 days in advance to advise of the outage. For any planned downtime less than an hour, an announcement is posted on the site for all users. All planned downtime is scheduled out of hours to minimise the impact on users.

Service Levels

There is user access to the LMS support desk which operates from Monday – Friday 9am to 5pm. Our support desk covers all areas of support including licencing issues, bugs/errors, technical help, enhancement requests and advice. They can be contacted via;

- Telephone on 0800 368 8549
- The contact form on the web site.
- Email support@linkmaker.co.uk

Set SLA's are defined for licenced users, during office hours notification that a support issue has been raised should be received within 2 hours.

Performance and Capacity monitoring are managed by our hosting provider and monitored 24/7. Any issues are escalated immediately, and remedial action taken. The LMS hosting provider has an average availability time of over 99.99%.

Financial Recompense Model for not Meeting Service Levels

Not applicable.

5. Provision of the service

Customer Responsibilities

For more information on customer responsibilities, please refer to the Terms and Conditions

Technical Requirements and Client-Side Requirements

Internet access is required for the web-based platform. The supported browsers are listed below.

- Safari
- Chrome
- Firefox
- Microsoft Edge
- Android
- Opera

Outcomes/Deliverables

LMS guarantees:

- Access to relevant functions the platform for the duration of the licence period
- Unlimited activity via an unlimited number of user accounts
- System availability and user support as detailed
- An ongoing development program keeping the platform aligned with national policies and procedures

Termination Process

The licence is purchased for a minimum period. Where the client wishes to stop using the services, we can restrict licenced features to an organisation's user.

Data extraction or deletion can be instigated by the user directly from the web site.

6. Our experience

Case Studies

Case study: finding a match for 2 siblings in Scotland

Ian Burdett, Senior Practitioner in the Community Resources Team at East Lothian Council, explains how Adoption Link helped find a family in England when no options within Scotland were identified.

East Lothian Council's usual means of family-finding includes use of the Scottish Adoption Register, as well as sharing the children's profiles with other Local Authorities and Voluntary Agencies near to us. We also attend Exchange Days, and occasionally use specialist publications- magazines and websites.

The family finding process started in earnest when our Agency Decision Maker ratified the plan for 2 siblings – aged 2 and 3 years old – to be placed for adoption, and a Permanency Order with Authority to Adopt was granted.

We were already aware that we did not have any suitable families in-house or within our consortium, and we also preferred to place the children out of the immediate area due to safety concerns. Our referral to the Scottish Adoption Register generated several initial enquiries, but these all withdrew once they heard that one of the children was significantly delayed in their development. A similar result was found when we approached the nearby Voluntary Agencies, and when we featured the children, UK wide, in a magazine.

- **We also had the option of hiding the children's profile, and inviting carefully selected adopters to view it**

We created profiles for the children on Adoption Link which included photos, and up-to-date information about the children. We found that being able to update this information - when needed - ensured that any adopters enquiring would always have up-to-the minute information.

We started with a Scotland-wide search, allowing all adopters registered on Adoption Link to view the profile. When no link was established, we started to look at LAs in the north of England. We later extended this further afield. We also had the option of hiding the children's profile and inviting carefully selected adopters to view it. We found that a significant number of potential links were identified, with three appearing to be particularly strong.

We settled on pursuing one link in the north of England and used Adoption Link to establish contact with the adopters and their social worker. We then shared information both ways (this can be done securely via Adoption Link), before visiting the family at their home. We then established a formal link, and the family were able to meet the children's paediatrician, and foster carers, before the family and children were matched. The move followed soon after this, with the adopters coming up to stay in a cottage for the first week of introductions, before the focus shifted to the adopters' home.

- **..family-finding through Adoption Link made a huge difference in this case, ensuring the children were able to find an adoptive family within a few hours travel of their foster care placement**

Both LAs liaised closely to ensure that the family and children were well supported throughout the process, and agreement was reached as to which LA would be responsible for the different aspects of support.

The children have settled extremely well. Both are now well established in their new family and thriving. Support has been put in place to ensure that the child with the most significant additional needs is having these needs met. We expect that the Adoption Orders will be granted soon, with the differences in legal processes between Scotland and England presenting little difficulty to date.

- **..social workers and adopters can be proactive in their efforts to link children and families, and can 'target' their efforts much more effectively**

We believe that family-finding through Adoption Link made a huge difference in this case, ensuring the children were able to find an adoptive family within a few hours travel of their foster care placement. We believe that the children may otherwise have needed to be placed with long-term foster carers.

One great advantage of Adoption Link is that both social workers and adopters can be proactive in their efforts to link children and families and can 'target' their efforts much more effectively - avoiding the delay caused by waiting for responses via telephone/e-mail, or pursuing links that could be quickly ruled out if more information were available.

Case study: finding a match early for 3 siblings

Ana Parr, Adoption Performance Lead at the London Borough of Bromley, explains how Link Maker helped reduce delay.

The London Borough of Bromley's normal means of family-finding includes the National Adoption Register, Link Maker, the different specialized magazines and their online services, as well as circulating the children's profiles with the other members of the Consortium and attending Exchange Days.

Using Link Maker has provided practitioners with the option of reaching out to potential adopters on the same day of the children's profile being typed up and added to the website. With the pressures to avoid delay for the children in care, Link Maker has helped us with instant publication of the material avoiding any time gaps.

- **With the pressures to avoid delay for the children in care, Link Maker has helped us with instant publication of the material avoiding any time gaps.**

Earlier last year, our Agency Decision Maker ratified the plan for 2 siblings – aged 5 and 18 months – to be placed for adoption. A couple of months later their younger sibling, who was 2½ months at the time, joined them, and the Agency Decision Maker approved the plan for the little one to be placed for adoption, together with his older siblings.

In Bromley, we had only placed one sibling group of 3 in the last 5 years and these children had been adopted by their foster carer. According to the Statutory Guidance on Adoption 2014, adoption agencies need to start family finding for children as soon as adoption becomes the plan. With that in mind we started family finding for the children around the time of an Issues Resolution Hearing.

We did not have any suitable families in-house or in the consortium at the time and we were unable to refer the children to the Register. We created anonymised, brief profiles of the children which we then used to start family finding.

- **Link Maker provided the option to look at the available families at any given time, using different search criteria.**

The only search available from the Adoption Register generated a very brief overview of families who were available, but without having the option of finding out more detail about these families. We were not able to look at the adopters' profiles before we referred the children to the Register, which we could not do without a placement order. Link Maker provided the option to look at the available families at any given time, using different search criteria.

We created an anonymised profile for the children on Link Maker in the summer of 2014. As we did not have legal consent to advertise the children, we carried out regular searches on Link Maker and approached families about the children.

Unfortunately, the families showed little or no interest in the children until a couple of months later, when the profile of a couple came up who wished to find out more. At this stage, we could not share much more than the initial profile, due to the case being in care proceeding and not wishing to pre-empt the outcome of court. The family had on some level made a connection with the children (all 3 together) without having seen any photographs of the children or knowing their real names. From the family's profile, we thought they could be a good match for the children.

The placement order for the children was granted late 2014.

While we were exploring this family, other families on Link Maker also expressed an interest in the children following their profile being updated and photographs uploaded late 2014, which provided us with other potential families that could also be considered for the children.

- **We believe that the early family-finding made a huge difference in this case, ensuring the timescale from placement order to placement was only 4½ months, with Link Maker providing the platform for this.**

We visited families very quickly after the final hearing. Information continued to be shared to ensure the families fully took on-board the likely challenges with such a large sibling group in very different stages of development and different levels of need. The match was taken to panel early 2015 and the children were placed at the end of March 2015, following well-planned introductions. The children have settled extremely well with their family.

We believe that the early family-finding made a huge difference in this case, ensuring the timescale from placement order to placement was only 4½ months, with Link Maker providing the platform for this

7. Clients



8. Contact details

Linda Hill – Director of Operations

linda@linkmaker.co.uk

Tel 0800 368 8549

Link Maker Systems Ltd

PO BOX 329

Bristol

BS15 0FF