

RA (Registration Authority) Policy

|  |  |
| --- | --- |
| Version number : | 6.0 |
| Consultation Groups  | Information Governance Steering Group |
| Approved by (Sponsor Group) | Information Governance Steering Group |
| Ratified by: | Quality Committee |
| Date ratified: | June 2022 |
| Name of originator/author: | Registration Authority Manager |
| Executive Director lead : | Chief Quality Officer |
| Implementation Date : | June 2022 |
| Last Review Date  | Feb 2022 |
| Next Review date: | June 2025 |

|  |  |
| --- | --- |
| Services  | Applicable  |
| Trustwide | X |
| Mental Health and LD  |  |
| Community Health Services  |  |

Version Control Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Author | Status | Comment |
| 1.0 | 09/12/2005 | Registration Authority Manager | Final | Approved by Registration Authority Project Board-03/11/2005Information Governance Committee-21/11/2005Clinical Governance Committee-14/11/2005Joint Staff Committee-08/12/2005 |
| 1.1 | 04/03/2010 | Registration Authority Manager | Final | Approved by Information Governance Steering Group |
| 2.0 | 19/12/2011 | Information Governance Manager | Final | Revised in line with Trust policy format requirements. Approved by IGSG-05/01/2012 |
| 2.1 | 08/05/2012 | Information Governance Manager | Final | Included section on RA security and maintenance |
| 3.0 | 15/03/2015 | Registration Authority Manager | Final | Revised in line with National RA Policy in line with Care Identity Service. National RA Policy using Care Identity Service (CIS) |
| 4.0 | 15/08/2018 | Registration Authority Manager | Final | Revised in line with Trust policy format requirements |
| 5.0 | 11/07/2019 | Registration Authority Manager | Final | Revised in line with New Processes and National RA Policy |
| 6.0 | 03/02/2022 | Registration Authority Manager | Draft | Revised in line with New Processes and National RA Policy. Page 13 Remote smartcard working emergency guidance |

**Contents**

|  |  |
| --- | --- |
| **Paragraph** | **Page** |
| **1.0** | **Introduction** | **4** |
| **2.0** | **Purpose** | **4** |
| 2.1 | RA/Care Identity Service | 5 |
| **3.0** | **Duties** | **6** |
| 3.1 | Registration Authority Manager | 6 |
| 3.2 | Registration Authority Agents | 6 |
| 3.3 | HR/Registration Agent ID Checkers | 7 |
| 3.4 | Local Smartcard Administrators | 7 |
| **4.0** | **Incident Reporting** | **7** |
| **5.0** | **RA Manager Reporting** | **8** |
| 5.2 | RA Agent Reporting | 8 |
| **6.0** | **Monitoring** | **8** |
| 6.1 | Audits | 8 |
| 6.2 | Smartcards | 8 |
| 6.3 | Smartcard Misuse | 8 |
| 6.4 | Revocation of Smartcards | 9 |
| 6.5 | Locum, Agency and Social Care Staff | 9 |
| 6.6 | Contractors | 9 |
| **7.0** | **Registration Authority Security and Maintenance** | **9** |
| 7.1 | Registration Authority Mobile Equipment Security | 10 |
| 7.2 | RA Forms | 10 |
| **7.3** | **Smartcards** | **10** |
| **8.0** | **References** | **11** |
| 8.1 | General Websites | 11 |
| **9.0** | **Associated Documentation** | **11** |
| 9.2 | Related Policies  | 11 |
| Appendices |
| A | Glossary  | 11 |
| B | Contact Details | 12 |

1. **Introduction**

The Registration Authority (RA) is a department within the Trust that ensures all
aspects of registration services and operations are performed in accordance with
National Policies and Procedures. The RA is responsible for providing arrangements
that will ensure tight control over the issue and maintenance of electronic
Smartcards, whilst providing an efficient and responsive service that meets the needs of the Users.

Healthcare Professionals need to be registered in order to ensure appropriate and secure access to Smartcard applications. The registration process for the National Programme has to meet the current national requirements. All NHS Digital applications use a common approach to security and confidentiality, based upon the NHS professional’s organisation/s, role/s, and business function (Activity). The method by which Users will be enabled to access an NHS Digital application is via a Smartcard issued during the Registration Process. A Registration Authority, which is required to conform to the

National Registration Policy, operates the Registration Process at a local level.

The East London Foundation Trust will comply fully with the latest published National

Policies and Procedures.

In Public Key Infrastructure (PKI) terms there is a single Registration Authority (the NHS Digital). All organisations that run a local Registration Authority do so on a delegated authority basis from the NHS Digital.

**2.0 Purpose**

The Registration Authority has the following responsibilities-

* Ensuring that the National Registration processes and any local processes developed to support the National Registration processes are adhered to in full
* Ensuring that there is sufficient availability of resource to operate the registration processes in a timely and efficient manner to meet the organisational responsibilities
* Ensuring that the RA team members are adequately trained and familiar with the local and national RA processes
* Ensuring that an indexed and secure audit trail of applicants registration information is maintained
* All documents (physical and electronic copies) are kept secure in an area which only the RA team can access.
* Ensuring RA Team members are familiar with and understand Registration

Policy and Practices for GPG45 level 3 or 4 Authentications, Registration Authorities Setup and Operation and this document

* Notification of the creation and revocation of RA Managers (including their email

address) to NHS Digital by sending an e-mail to ramanagers.agents@nhs.digital.gov.uk

* Ensuring that there are sufficient Smartcards and Smartcard issuing bodies

and maintenance equipment for the organisation. Note: see

NHS Digital RA Hardware Ordering Process

The Trust Registration Authority is made up of the following personnel:

* Registration Authority Manager
* Registration Agents
* Registration Authority ID Checkers
* Local Smartcard Administrators

The services available are:

* User Registration
* Issuance of Smartcards
* Role Profile maintenance
* Revocation and cancellation of Smartcards
* User Suspension
* PIN/Passcode resetting
* Smartcard renewal and exchange

The above services will be available during the Trust Registration Authority Service

Core hours, 08:00 to 16:00 Monday to Friday, not bank holidays. Local Smartcard Administrators are available in each Directorate to unlock/reset blocked/ cards or forgotten passcodes and Users can now register to unlock their own Smartcards.

**2.1 RA/Care Identity Service (CIS)**

*Background*

This document outlines:

* The RA Hierarchy and the principle of delegated authority to local organisations to run their RA.
* The requirements for creating a nationally verified digital identity.
* The roles and responsibilities within organisations that run their own Registration Authority activity.
* Requirements in relation to Smartcards.
* The requirement to develop and implement a local RA Policy.
* CIS simplifies the registration process for issuing Smartcards.

*Purpose*

To align Registration Authority with the National RA Policy using CIS to reduce the use of paper forms to create a digital identity.

**3.0 Duties**

All Trust RA staff will have sufficient training to carry out their RA tasks in accordance
with National Policies and Procedures. They will be individuals capable of trust, as they will be handling sensitive information covered by General Data Protection Regulations.

They will be key players in ensuring the NHS Code of Confidentiality and the NHS Digital Acceptable Use Policy, Terms and Conditions is followed.

The name of the Board/EMT accountable person and the RA Manager must be named within the policy.

Senior Information Risk Owner (SIRO)

RA Manager

**3.1 Registration Authority Manager**

The RA Manager is accountable to the Trust Executive and is responsible for the set up and day to day running of the Trust RA service. Responsible for running the RA Governance in their Organisation and cannot delegate this. The RA Manager must ensure:

* that all RA procedures are carried out in accordance with local and national policy
* Facilitate the process for agreeing the organisation’s access control positions.
* Appropriate auditing is carried out.
* Operational security of (old) paper based RA records.
* Users ID checked to GPG45 level 3 or 4.
* Users are compliant with the terms and conditions of Smartcard usage and that issues are raised appropriately locally and nationally.
* Responsible for training all other RA staff who will conduct ID checking to ensure that appropriate standards exist and they can evidence good ID checking.
* RA Agents are registered.

 **3.2 Registration Agents**Registration Agents are responsible to the RA Manager for ensuring that the National and local processes are followed. They are responsible for:

* The issue of Smartcards and checking staff credentials at a face to face meeting.
* Id checking to GPG45 Level 3 or 4-NHS Employers check standard and recording it on the Electronic Staff Record (ESR) or CIS. This provides assurance that the identity is valid across any organisation an individual works within. This also applies to core identity attribute changes (Name, Date of Birth or National Insurance Number). Grant external Users access, renew certificates if expired.
* Ensuring Users accept terms & conditions of Smartcard use when registering them.

All incidents, misuses, anomalies and problems will be reported to the RA Manager. Smartcards can only be issued to individuals who have a national verified digital identity.

**3.3 HR/Registration Agent ID Checkers**
HR/Registration ID checkers are responsible to the RA Manager for ensuring that the National and local processes are followed. They are responsible for Id checking to GPG45 level 3 or 4 /NHS Employers check standard and recording it on the Electronic Staff Record (ESR) at a face to face meeting. This also applies to core identity attribute changes (Name, Date of Birth or National Insurance Number). This provides assurance that the identity is valid across any organisation an individual works within. Smartcards can only be issued to individuals who have a national verified digital identity.

**3.4 Local Smartcard Administrators (LSA)**Local Smartcard Administrators are responsible to the RA Manager for ensuring that National and local processes are followed. These administrators will normally be accessible Users within a work area. The list of these administrators will be published on the Trust Intranet. The LSA should ensure that they have sufficient staff to provide cover across all working patterns within a work area. For example if the service is 24 hours there should be an LSA available on all shifts. Staff can now unlock their own Smartcard and are given guidance on how to register for this process. Also available on the ELFT intranet.

**4.0 Incident Reporting**

Incidents should be reported, using the Trust’s Incident Reporting Procedure (Datix), and to the RA Manager.

Examples of incidents are:

* Smartcard or application misuse
* Smartcard theft
* Non-compliance of local or national RA policy
* Any unauthorised access of NHS Digital Health applications
* Any unauthorised alteration of patient data on NHS Digital applications
* Any unauthorised access of other Smartcard enabled systems
* Lost/damaged Smartcards should be reported via the IT Service Desk Portal rather than raising a Datix

Identity checking must be carried out by those holding an RA role – RA Managers and the RA Agent/RA Agent ID Checker roles.

The RA manager will consider all reported incidents. Any incidents considered

Significant, will be reported to the Information Governance Manager depending on the nature of the incident, may result in action being taken against an individual, in accordance with Trust policy.

Only the end user for whom the Smartcard is intended should know their passcode for their Smartcard, no-one else should, including RA staff. If anyone else knows the end Users passcode it breaches the Smartcard terms and conditions of use and the Computer Misuse Act 1990.

It is mandatory that Users sign the Terms & Conditions of Smartcard use. This reminds them of their responsibilities and obligations, including not sharing the card, leaving the card unattended, and not disclosing their passcode to others.

RA staff (RA Managers, Advanced RA Agents and RA Agents), are reminded that it is their responsibility to ensure that Users comply with these terms and conditions.

A major breach of security will also be reported by the RA manager to the LSP and

NHS Digital

* to ensure any risks resulting from the event can be taken into account and mitigated against.
* a significant incident is an isolated incident or a series of less significant incidents

that could lead to a serious degradation of healthcare or information security. The

RA Manager and Information Governance Manager will consider incidents reported

to them and decide whether Trust systems or working practices should be reviewed

as a result.

* documentation will be kept by the RA Manager and/or on the HR file as appropriate.

**5.0 RA Manager Reporting**

The RA Manager will report significant incidents to the Information Governance Manager in accordance with the Incident Reporting Policy.

**5.2 RA Agent Reporting**

Registration Agents will report any RA related incidents, using theTrust Incident Reporting Procedure and to the RA Manager. Additionally RA Agents will report any operational difficulties in using CIS/Spine compliant systems (especially where these have patient healthcare implications) to the RA Manager.

**6.0 Monitoring**

**6.1 Audits**

All RA functions will be regularly audited by the RA Manager and will be results will be reported to the Information Governance Steering Group (IGSG), including

 The issue of Smartcards

 The management of Smartcards

 The profiles associated with Users in relation to what they do

 The use of Smartcards

 The use of NHS Digital/Trust applications

 Identity management

 Security of supplies and equipment

**6.2 Smartcards**

Smartcards should be treated with care and protected to prevent loss or damage. All

Users should adhere to the latest Terms and Conditions guidance given when the

card was issued and any subsequent guidance. Spot checks should be carried out by the RA Manager on a regular basis to ensure Terms and Conditions are adhered to and reported to the IGSG.

**6.3 Smartcard Misuse**

Staff members are responsible for reporting suspected Smartcard misuse in line with

Trust’s Incident Reporting Policy. In serious cases the certificate associated with the

Smartcard may be suspended or revoked, and disciplinary action will be taken.

**6.4 Revocation of Smartcards.**

If the User is an East London NHS Foundation Trust (ELFT) employee and is moving to another NHS organisation, the Smartcard access is automatically revoked through the staff record. Non ELFT - External staff must have an end date put on their user profile when creating ELFT access. This will be a maximum of 1 year Agency Staff. A User moving to another NHS organisation should retain the Smartcard for use in the new organisation. If they leave the NHS permanently, the Smartcard Certificates will be revoked.

There are other occasions when it is necessary to deactivate a Smartcard by

cancelling or revoking the Smartcard certificate. Reasons for this include:

* The Smartcard has been lost or stolen
* There has been some other security breach associated with the Smartcard or Smartcard certificate.
* The card has become damaged

The RA Manager authorises the revocation of a card in consultation with the HR Manager, as appropriate.

Revocation renders the Smartcard useless, whereas deactivation removes all access to the system allowing the card to remain valid.

**6.5 Locum, Agency, Honorary and Social Care Staff**

* Temporary, Locum, Agency, Honorary and Social Care staff may have a legitimate need to gain access to NHS Digital Health records as part of their role. The following points should be considered: Staff working as part of a team may not need a Smartcard to fill the role
* Some staff could already be registered and will only require a role profile

added for use at ELFT.

* Line managers should be aware that temporary staff who are Smartcard

holders may not have sufficient training in the use of the particular NHS Digital Application. All staff will be trained in an application before being allowed to access data.

* Locum and Agency staff need to complete a request on the IT Service Desk Portal to register for a Smartcard or access to a clinical system. Access will be assigned for 1 year and recorded by the RA team. Notification will be sent to the user, to inform them that their access will need updating.
* Honorary and Social Care staff will need an honorary contract set up with the placements team in HR. This will then generate a request for the RA team to print a Smartcard.

All applicants will need to provide all the correct identification documentation, regardless of the contract they have with the Trust eg: permanent or bank. The relevant senior manager for the Directorate will be responsible for authorising the necessary access.

All temporary staff including locum, agency, Social Care staff will be bound by this policy and other related Trust policies on security and confidentiality of information.

**6.6 Contractors**

The Trust will ensure all contractors who need to use the NHS Digital applications are bound by the General Data Protection Regulations and NHS Digital Confidentiality Code of Practice. This will include the process to be taken in cases of a breach and liability issues.

The Trust will ensure that all contractors sign a confidentiality agreement as part of

their contractual arrangements.

**7.0 Registration Authority Security and Maintenance**

The RA Manager is responsible for ensuring that adequate numbers of Smartcards

are available, and will maintain the Smartcards throughout their useful life. The

Associate Director of ICT will ensure that there is sufficient computer equipment to

support all Users of NHS Digital applications (including those for

registration) containing the latest software. All RA equipment will be subject to

policies and procedures governing the management and control of Trust Assets.

**7.1 Registration Authority Mobile Equipment Security**

Mobile RA equipment must be locked in a secure area at all times when not in use.

Any incident relating to the loss or theft of RA equipment or documentation should be reported to the RA Manager immediately so that adequate security measures can be taken and the incident logged on Datix.

**7.2 RA Forms**

RA Forms will no longer be used for CIS Registration/assigning access, but any paper records/scanned copied must be kept in accordance with the national guidance – for 6 years or until the person’s 70th birthday.

RA - online Forms

There will be a form on the IT Service Desk Portal for external staff to apply for a Smartcard or for access to be assigned to ELFT. The agency/locum worker will then be contacted by the Registration Authority to have an Identity check to GPG45 Level 3 or 4 and be issued a Smartcard. An end date (Maximum 1 year) for the access for external staff must always be entered on CIS. If an external user is leaving the Trust but is moving to another NHS organisation the card should be retained by the user.

*Revoked access*

The Smartcard access will automatically be revoked in the case of the following as access is controlled by the staff record:

 Staff suspension pending disciplinary investigations

 Maternity leave

 Long term sick leave

 Secondment

**7.3 Smartcards**

*Name on Smartcards*

The name registered on CIS is controlled by the name which is on the photographic evidence supplied ie: Passport/Driving Licence, but a preferred name can be printed on the Smartcard.

The Trust Name is not printed on Smartcards, as the cards are transferable between all NHS organisations*.*

*Lost, Stolen and Broken Smartcards*

Lost and damaged Smartcards should be reported to the RA/Smartcard Team via the IT Service Desk Portal as soon as is practicable*.*

In the case of theft the RA Manager must be informed so that checks may be made

to ensure that the Smartcard has not been misused and the incident logged on Datix.

**8.0 Remote smartcard registration – emergency guidance for Registration Authorities**

**Guidance for Registration Authority (RA) service providers and Registering Organisations when completing RA smartcard registrations using video conference facilities.**

**This process will apply when face-to-face registration meetings and the use of identity checkers are not possible during the Coronavirus (COVID-19) pandemic.**

## About the process

This process applies, until further notice via revised guidance, to all registrants, where a face to face meeting is not possible.

During the coronavirus (COVID-19) pandemic, [it replaces the standard registration process](https://digital.nhs.uk/services/registration-authorities-and-smartcards) and involves a method of establishing the registrant’s identity through the remote provision of:

* [identity document](https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual)
* an image file suitable for use as a passport-compliant photograph
* confirmation that the image is a true likeness of the registrant

This process is to be used by Service Provider Registration Authority (RA) Agents acting on behalf of Registering Organisations whenever they need to register a new member of staff.

It allows for user access to be rescinded and/or users de-registered in a managed way when normal conditions return.

## Prerequisites

Registration Authority (RA) Service Providers will:

* distribute this guidance to the relevant staff in all organisations for which they have registration responsibilities
* agree with their Registering Organisations the appropriate video conference channel(s) for video calls (VCs) taking into account availability, security and cost - possible channels include [Microsoft Teams](https://products.office.com/en-gb/microsoft-teams/group-chat-software), [Slack](https://slack.com/intl/en-gb/), [Zoom](https://zoom.us/), [Webex](https://www.webex.com/), [Jabber](https://www.cisco.com/c/en/us/products/unified-communications/jabber/index.html) and [FaceTime](https://support.apple.com/en-gb/HT204380)
* agree with their Registering Organisations appropriate locations that they will allow when registering for their organisations - locations need to be sufficiently private, for example registrants' homes
* ensure that their Registration Authority staff are aware of these procedures and the specific arrangements with the organisations for which they have registration responsibilities

## Remote registration process - stage 1 (before the video call)

The Registration Authority (RA) Agent for the Registration Authority (RA) Service Provider receives a request for [smartcard registration](https://digital.nhs.uk/services/registration-authorities-and-smartcards) via existing channels and processes. It is essential that the registrant provides their email address, preferably an NHS or other secure email address if available. Otherwise judgement is to be exercised by the Registration Authority (RA).

In response to the registration request, the Registration Authority (RA) Agent asks the registrant to provide the following items by email, again, by [NHSmail](https://portal.nhs.net/) or other secure email if available:

* organisation for first registration (if not already specified in the request)
* full name
* date of birth
* national insurance number
* scan of one photographic identity document(s) - needs to be a valid passport or driving licence
* image file suitable for use as a passport-compliant photograph
* mobile phone number (required later to text the smartcard passcode)

In the email, the Registration Authority (RA) Agent gives the registrant their mobile number to confirm the receipt of the smartcard and receive its passcode once posted.

In the unlikely event that the registrant does not have any photographic identity documents the Registration Authority (RA) Agent will decide which document(s) from the NHS Employers options (for users with no photographic ID) should be asked for.

Once the required documents have been received, the Registration Authority Agent contacts the Registrant to arrange the video meeting and explain the process.

## Remote registration process - stage 2 (the video call)

The Registration Authority (RA) Agent:

* text messages a set of [randomly generated numbers](https://www.random.org/integer-sets/) each time to the registrant who is asked to read it out - this binds the telephone number to the individual on the video call and establishes the number to text the smartcard passcode to (see below)
* asks the registrant to show their scanned photographic identity document for the Registration Authority (RA) Agent to check against the live image of the registrant

Assuming that the video call image of the registrant matches the image on the scanned identity document, the video call process is complete, and the Registration Authority (RA) Agent can terminate the video call and continue the registration process.

## Remote registration process - stage 3 (after the video call)

The Registration Authority (RA) Agent creates/completes the registrant’s identity in the [Care Identity Service (CIS)](https://digital.nhs.uk/services/registration-authorities-and-smartcards/care-identity-service).

In order to flag the entry as a COVID-19 record the Registration Authority (RA) Agent enters the following data:

* choose UK passport as the photographic evidence – enter 000000000 in the passport number field and the date 1 April 2025 in the expiry date field
* go to non-photo ID and select ‘TAC1’ and ‘TAC2’ (Temporary Access Card) as the two sources of non-photo ID (used for creation of temporary access cards in other situations) and enter 1 March 2020 as date of issue

The Registration Authority Agent:

1. prints the smartcard for the registrant, unlocked with a randomly generated 6-digit passcode obtained from a service such as https://www.random.org/integer-sets/, and records the passcode securely.
2. arranges for delivery of the smartcard to the registrant.
3. texts the smartcard’s 6-digit passcode to the registrant (using the registrant’s previously recorded mobile number), when they call to say that the smartcard has been received.
4. assigns access to the registrant using the normal process.

## Additional information

### What to do if an existing user locks their card or the certificates expires

Without face to face contact the only option is to print a new unlocked card as per process above and send to the user – and cancel the locked or expired card.

### What happens when you need to rapidly move pharmacy staff to other pharmacies

It has been agreed that wider use of the Role Based Access Control (RBAC) 'National Locum Pharmacy Agency' code and position (FFFFF) can be used, but it is important that RAs keep a log of users given this access for exceptional reasons so that it can be revoked as appropriate at some point in the future.

**9.0 References**

**9.1 General Websites**

<https://digital.nhs.uk/Registration-Authorities-and-Smartcards>

**10.0 Associated Documentation**

**10.1 Related Policies and Processes**

The Trust will ensure that processes supporting the identification, registration and

management of staff will be integrated with other policies and processes within the

Trust as appropriate*.*

**11.2 Trust Policies**

<http://elftintranet/sites/common/private/search_quick21.aspx?q=information%20governance%20policy&orderby=0&url=ObjectInContext.Show(new%20ObjectInContextUrl(2%2C29769%2C1%2Cnull%2C970%2Cundefined%2Cundefined%2Cundefined%2Cundefined%2Cundefined))%3B>

**Appendix A**

**GLOSSARY**

**NHS Digital**

Formerly known as Health and Social Care Information Centre

**Local Service Provider (LSP)**

Local Service Provider of Information Technology

**National Care Records System (NCRS)**

National IT System storing patient care records

**Pass-code/PIN**

The digit entered into the computer when logging onto the system. This allows the

system to know that the person using the Smartcard is the person whose Smartcard

it is. *This should only be known by the User*

**Registration Authority (RA)**

The Registration Authority ensures that all aspects of Registration adhere to National

Policies and Procedures. It is also responsible for ensuring tight control over the

issue of Smartcards and the security of information

**RA Agent**

RA Agents are responsible for checking candidates’ credentials and issuing

Smartcards

**RA Agent ID Checker only**

RA/HR are responsible for checking candidates’ credentials and recording on the Electronic Staff Record (ESR)

**Position Based Access Control (PBAC)**

Positions are created then assigned through the staff record for ELFT staff and by the RA Agent/Manager for non ELFT staff ie: Agency/Locum. The position denotes which access/system is available to the User

**Smartcards**

The cards used to gain access to the relevant systems with an electronic chip.

These have the Users’ name and photograph printed on them, but not the name of

an Organisation, as they can be transferred from Trust to Trust

**Care Identity Service**

Where information is held on all Users nationwide

**User**

Staff members who have Smartcards and use the associated systems

**Unique User ID Number (UUID Number)**

The Unique User Identifying number assigned to each User

**Workgroup**

Set up for groups of people to work in different areas of patient care to view records as long

as they have a legitimate relationship to do so

**Appendix B**

**Contact Details**

**Registration Authority (Smartcard) Team via The IT Service Desk Portal or Telephone: 0207 655 4004**

**Address**:

Robert Dolan House

Alie Street

London

E1 8DE