Greater Manchester Shared Services

GMSS Subject Access Requests Policy

Review Date: February 2022

Document Control

Title / Reference:	Subject Access Request Policy
Status:	Approved
Version:	V2.5
Date Issued / Ratified:	March 2020
Originator of Document and Job Role:	IG Team
File Classification:	Official Data
Retention:	Life of the organisation plus 6 years (place of deposit)
Target Audience:	All GMSS staff & 3rd party partners
Links to other strategies, policies, procedures etc:	• Data Security, Protection & Confidentiality Policy • Data Security, Protection & Confidentiality Framework • Confidentiality Audit Procedure • Data Security Breach & Incident Reporting Policy • Secure Transfer of Data Policy • Acceptable Use of IT / Information Systems Policy • Information Classification Policy • Records Management Policy • Risk Management Policy • Information Risk Policy • Subject Access Request Policy • Registration Authority (Smart Card) Procedure • Data Security, Protection & Confidentiality Staff Handbook **This list is not exhaustive**

Change History

Summary of Changes	Name	Date	Version
Reviewed by SMT IG	IG SMT	Oct 13	1.0
Added Access to health records Act information	LW	May 14	1.1
Reviewed	LW	Aug 14	2.0
Removed section on fees and updated generic SAR email address	JW	Apr 15	2.1
Reviewed and amended	Head of IG	Sept 15	2.2
Reviewed for re-approval	IG	Aug 16	2.3
Reviewed to document changes in line with GDPR	IG Team	May 17	2.4
Reviewed – updated timescales	IG Team	Nov 19	2.5
Updated to Policy from Procedure, rewording to make Policy clearer	IG Team	Feb 20	2.5

Review

Name	Role	Date	Version
IG SMT	IG SMT	2014	2.0
SMT	SMT	Aug 16	2.3
IG Group	IG Group	Dec 17	2.4
IG Group	IG Group	Feb 20	2.5
Governance Committee	Governance Committee	Mar 20	2.5
Senior Management Team	Senior Management Team	Mar 20	2.5

Approval

Name	Role	Date	Version
IG SMT	IG SMT	2014	2.0
SMT	SMT	Aug 16	2.3
IG Group	IG Group	Dec 17	2.4
IG Group	IG Group	Feb 20	2.5
Governance Committee	Governance Committee	Mar 20	2.5
Senior Management Team	Senior Management Team	Mar 20	2.5

Distribution

Name	Role	Date	Version
Saved in policy folder		Dec 17	2.4
Updated policy tracker		Dec 17	2.4
Saved in policy folder		Nov 19	2.5
Updated policy tracker		Nov 19	2.5
GMSS Publication scheme		Mar 20	2.5
The Bulletin		Mar 20	2.5
People Matters		Mar 20	2.5

DOCUMENT STATUS:
This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of the document are not controlled

Contents

Appendices

1. Introduction

The Data Protection Act / General Data Protection Regulation (GDPR) gives every living person (or their authorised representative) the right to request access to information held about them by an organisation irrespective of when it was compiled.

Access to deceased patient's information is governed by the Access to Health Records Act 1990. A record can be computerised (electronic) and / or manual form (paper files). It may include such documentation as hand written notes, letters to and from other professionals, reports, imaging records, printouts, photographs, DVD and sound recordings.

Subject Access Requests (SAR) relating to Greater Manchester Shared Services (GMSS) will normally be for access to view and / or to request copies of the following types of records which GMSS process:

- HR records and other related HR documents for GMSS staff held by GMSS People Services.
- Internal correspondence about a staff member could be requested under the Data Protection Act / GDPR as a subject access request.

GMSS do not process original health records. If requests for health records are made, the requester will be asked to contact the data controller which will either be the GP and / or a secondary care NHS Trust.

It is important that all staff bear in mind when compiling records that the content could be requested under the Data Protection Act / GDPR as a subject access request, and ensure that records they create are written in a way that would be appropriate to disclose.

2. Purpose & Scope

This policy informs staff how requests for access to information about an individual are dealt with and how GMSS respond to such requests. It explains the process by which patients; members of the public; staff; legal representatives and 3rd parties can request the information.

This policy is designed to provide a guide to best practice in handling requests but guidance should be sought from the Information Governance (IG) Team. Full implementation of this policy will enable the organisation to:

- Comply with legal obligations under the Data Protection Act / GDPR.
- Increase levels of trust and confidence by being open with individuals about the information that is held about them.
- Provide better customer care.
- Improve transparency of organisational activities in line with public policy requirements.
- Enable individuals to verify information help about them is accurate.

This policy applies to:

- Members of staff directly employed by GMSS and for whom GMSS has legal responsibility.
- Staff covered by a letter of authority / honorary contract or work experience.

- All third parties and others authorised to undertake work / process data on behalf of GMSS.

3. Responsibilities & Definitions

Roles & Responsibilities

Managing Director

The Managing Director has overall responsibility for Data Security & Protection within GMSS. As Accountable Officer, they are responsible for the management of Data Security & Protection and for ensuring appropriate mechanisms are in place across the entire organisation (GMSS) to support service delivery and continuity. Information Governance provides a framework to ensure that information is used appropriately and is held securely.

Caldicott Guardian

The Caldicott Guardian is the conscience of the organisation and is responsible for ensuring that national and local guidelines on the handling of confidential personal information are applied consistently across the organisation. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

Senior Information Risk Owner (SIRO)

The SIRO takes ownership of GMSS's information risk framework. As a member of the Senior Management Team, the SIRO acts as an advocate for information risk and provides written advice to the Managing Director on the content of their annual governance statement in regard to information risk.

Data Protection Officer (DPO)

The DPO informs and advises staff about their obligations to comply with GDPR, the Data Protection Act and other relevant legislation. The DPO monitors GMSS's compliance with data protection policies and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities.

Heads of Service

Heads of Service take responsibility for ensuring that the Data Security, Protection & Confidentiality framework is communicated and implemented within their service, and ensure that all staff remain compliant, including any temporary or contract staff.

Information Asset Owner / Administrator (IAO / IAA)

The IAO / IAA are responsible for ensuring that specific information assets are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited.

IG Team

Responsibility for the management of Subject Access Requests lies with GMSS Information Governance team. This includes:

- Log the request on the Subject Access Request log.
- Acknowledge the Subject Access Request to the requestor.
- Request ID if applicable and complete ID checks.
- Collate the information, contacting HoS/Service Leads for the information.
- Refusing any requests if applicable.
- Finalised response to the requestor and send all information with a covering letter detailing what has been sent.
- Respond to any further clarifications from the requestor.
- Close the request.
- Monitor Subject Access Requests and report to the IG Group.

Head of Corporate IT & IT Security Manager

The Head of Corporate IT and IT Security Manager are responsible for ensuring that all GMSS electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations.

All staff

All staff, whether permanent, temporary or contracted, working in a clinical or non-clinical environment are responsible for ensuring that they are aware of the Data Security & Protection requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

All staff have a responsibility to ensure they complete the mandatory training requirements of the organisation. Data Security & Protection are part of these mandatory training requirements.

Definitions

Data Controller

Under the Data Protection Act / GDPR, GMSS is the data controller. That is, the organisation (or person) that determines the purposes for which and the manner in which any personal data about individuals is processed.

Data Subject

According to the Data Protection Act / GDPR, the data subject is a living individual (not an organisation) who is the subject of the personal data.

4. Recognising a Subject Access Request (SAR)

A Subject Access Request (SAR) is any request made by an individual or an individual's representative (see Rights of Access section) for information held by GMSS about that individual.

A SAR can be made in a number of ways (listed below), however, the requestor does not need to mention the Data Protection Act or GDPR legislation in their request. They need to state that they are making a SAR for their request to be valid. They may even refer to other legislation, for example, the Freedom of Information Act 2000, but their request should still be treated according to this policy. GMSS IG Team has a form called "Request for Access to personal information form" which can be provided to a requestor to submit a subject access request. A copy of this can be found in

Appendix 1.

A Subject Access Request can be made via any of, but not exclusively to the following methods:

- Email
- Post
- Corporate website
- Verbally - the requestor can verbally request a SAR which would then be followed up by us in writing, to ensure there is a record of the request.

Subject Access Request's made online must be treated like any other SAR when they are received. However, GMSS will not provide personal information via social media channels.

Subject Access Requests should be identified and forwarded immediately to the GMSS IG Team, who will then co-ordinate the request and contact the Information Asset Owner to process the request. The IG Team contact details are:

Information Governance – Subject Access Requests
Ellen House
Waddington St
Oldham
OL9 6EE

Tel: 0161 290 4911
Email: gmss.sar@nhs.net

5. Rights of Access

Under the Data Protection Act / GDPR, any living person, who is the subject of personal information held and processed by GMSS, has a right to request access to that information. This is a legal right, subject to given exemptions (see section 7). They also have the right to an explanation of any terms they may not understand (such as technical language or terminology) and the right to ask that any inaccurate information is corrected, and to request a copy of those corrections.

Subject access provides a right for the subject to see / view their own personal data as well as to request copies of these.

An individual does not have the right to access information recorded about someone else, unless they are an authorised representative, or have parental responsibility.

GMSS is not required to respond to requests for information unless it is provided with sufficient details to enable the location of information to be identified, and to satisfy itself as to the identity of the individual making the request. If a request is made verbally, the IG Team will confirm this in writing via post or email.

6. Requests from Parties other than the Subject

Requests for access to records made by a patient representative

Any person can authorise a representative to request to access information held about

them on their behalf. This must be completed in writing, with confirmation of the representative's identity and relationship to the patient.

Representatives able to provide evidence that they are acting under a Power of Attorney or a Court of Protection Order will be granted access to information held about an individual.

Where an individual who is physically or mentally disabled and unable to provide written consent for a representative to seek access on their behalf, GMSS will give the individual as much assistance as possible, in order to ascertain whether consent has been granted by other means to the representative.

Request for access by other organisations

Where access to the records is being requested for any purpose other than Subject Access, advice should be sought from the IG Team.

Parental rights of access & parental responsibility

Parents, or those with parental responsibility, will generally have the right to apply for access to information held about a child. Disclosure may be refused if the child is deemed competent as "Gillick competent" and refuses to give consent. For further information regarding parental rights of access see the link below:

https://www.nhs.uk/using-the-nhs/about-the-nhs/how-to-access-your-health-records/

Parental responsibility is defined in the Children Act 1989 as 'all the rights, duties, powers, responsibilities and authority which by law a parent of a child has in relation to the child and his/her property'.

Married parents both have parental responsibility, unless a Court Order has removed that status from any party. A separated or divorced parent who no longer lives with the child has parental responsibility unless a Court has removed that status from either party.

Parental responsibility endures if the child is in care or custody. It is lost, however, if the child is adopted.

If the parents are not married, only the mother automatically has parental responsibility. The father may acquire it in the following ways:

- Registering the birth, along with the mother, as the child's father (for children born after 1st Dec 2003).
- Formal agreement with the mother (Section 4 of the Children Act 1989) - agreement can then only be brought to an end by a Court.
- Marrying the mother.
- Obtaining a Court Order.
- Obtaining a Residence Order.

Parental responsibility can also be acquired:

- Through appointment as the child's guardian.
- By way of a Residence Order from the Court.
- By anyone having an Adoption Order made in their favour.

Through Section 2(9) of The Children Act 1989 – "A person who has parental responsibility for a child may not surrender or transfer any part of that responsibility to another but may arrange for some or all of it to be met by one or more persons acting on his behalf", a Local Authority can acquire parental responsibility by:

- Emergency Protection Order (local authority).
- Interim or Full Care Orders (local authority).

In this case the parents do not lose parental responsibility but the local authority can limit the extent to which a person exercises their parental responsibility.

In practice, parental responsibilities would include:

- Safeguarding a child's health, development and welfare.
- Financially supporting the child.
- Maintaining direct and regular contact with the child.

Where, in the view of a health professional, the child is not capable of understanding the application for access to records, GMSS is entitled to deny access as being against their best interests.

Legally, young people aged 16 and 17 are regarded to be adults for the purposes of consent to treatment and the right to confidentiality. As such, if a person of this age wishes any information about them to be treated as confidential this wish should be respected and they have the right to deny parental access to information held about them.

7. Exemptions

Disclosure might cause harm / third party information

Under the Data Protection (Subject Access Modification) Health Order 2000 / GDPR, GMSS has the right to deny access to all or part of records if one of the following conditions applies:

- If, in the opinion of the healthcare professional / Head of Service, access would disclose information likely to cause serious harm to the physical or mental health or condition of the patient or any other person (for example, a child in a child protection case).
- If giving access would disclose information which identifies a third party (unless the individual concerned has given consent).

Those who make the disclosure decision (e.g. Healthcare Professionals / Head of Service) must carefully consider, and be prepared to justify, any decisions to disclose or withhold information. The Caldicott Guardian and / or SIRO must be advised if there appear to be any grounds for withholding information.

If information has been withheld, GMSS is free to advise applicants of the grounds on which information has been withheld – but they are not obliged to do so. For example, GMSS may not wish to volunteer the fact that information has been withheld if they believe that such a disclosure would cause undue distress, or if it might jeopardise a child protection investigation.

Child protection / safeguarding concerns

There may be situations in which access to all or part of a child's health records can be refused to a requestor – for example, where there are on-going child protection issues, or where releasing information may put a child or young person at risk of harm. In these cases, advice must be sought from the appropriate managers and child protection / safeguarding professionals, as well as the Caldicott Guardian and / or SIRO, before releasing any information.

Third party disclosures

Where records contain information that relates to an identifiable third party, that information may not be released unless:

- The third party is a health professional who has compiled or contributed to a health record, or who has been involved in the care of the individual.
- The third party, who is not a health professional, gives their written consent to the disclosure of that information.
- It is reasonable to dispense with the third party's consent (taking into account the duty of confidentiality owed to the other individual, any steps taken to seek his/her consent, whether he/she is capable of giving consent and whether consent has been expressly refused).

Excessive requests / Manifestly unfounded

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

- Charge a reasonable fee taking into account the administrative costs of providing the information; or
- Refuse to respond.

If a decision is made to refuse to respond to a request, then without undue delay and within one month of receiving the request you should inform the requestor that:

- You believe the request is manifestly unfounded or excessive.
- The requestor has the right to complain to the Information Commissioners Office (ICO).
- The requestor is entitled to seek to enforce the right of access via the Courts.

Information relating to the deceased

Applications for access to health records of the deceased are made under the Access to Health Records Act 1990. Records made after 1st November 1991 can be made available to a patient representative, executor or administrator. Any person with a claim arising from the death of a patient has a right of access to information specifically relating to the claim.

The person making the request must explain why they need access to the records and which part of the record supports their claim.

The request should normally be made to the last known record holder, unless there are extenuating circumstances, such as concerns over the treatment the deceased person received. In such cases, advice must be sought from the Caldicott Guardian.

Dealing with joint records

Where joint records are held, the relevant organisations must be informed of the access request and agree who will lead the disclosure process. However, requests for joint records should not have to be made to both organisations. Either organisation can provide the information requested provided the applicant is informed that the information is jointly held.

The term 'joint records' does not include records that contain information provided by one organisation to the other. While the information held by each organisation might be similar, they cannot be considered as joint records. In such cases a separate application must be made to each authority.

8. Subject Access Request Process

Appendix 3 provides a map of the process for dealing with Subject Access Requests.

The Key steps can be summarised as follows:

- **Receipt of request** – Requests for information held about an individual must be directed to the IG team via gmss.sar@nhs.net , who will acknowledge the request and log it on the Subject Access Request log. They will also notify the requestor of the next steps. The requestor may be asked to complete a form to better enable GMSS to locate the relevant information. GMSS IG Team will forward the relevant form to the requestor, see Appendix 1.

- **Confirmation of identity / further clarification**– If ID and clarification of a subject access request has not already been provided, GMSS IG Team will ask the requestor to provide 2 forms of ID, one of which must be a photo ID and the other confirmation of address. See Appendix 2 for a full list of ID that may be provided. ID can be photocopied but this must be certified and posted to GMSS or it can be scanned and emailed to GMSS. ID must be certified with the following statement "I cerifity that this is a true likeness of [title and full name of requestor]". They must add their signature and date under the statement. The person certifiying copies of ID must:

    - have known you (or the adult who signed the form if the passport is for a child under 16) for at least 2 years;
    - be able to identify you, for example they're a friend, neighbour or colleague (not just someone who knows you professionally);
    - be 'a person of good standing in their community' or work in (or be retired from) a recognised profession.

- **Confirmation** – Once the ID /clarification have been received, GMSS IG Team will confirm this to the requestor and notify them that their request will be responded to within a month. The period begins from the date that the ID/clarification/fees are received. The requestor will be informed if there will be any deviation from the 1 month timeframe. Any deviation from the timeframe should be an exception and be escalated to the Caldicott Guardian and / or SIRO for approval prior to informing the requestor.

- **Collating** – GMSS IG Team will contact and ask the relevant Head of Service for the information requested and provide deadlines for the response. It is up to

the Head of Service to advise GMSS IG Team of any reason why information cannot be released to the data subject. GMSS IG Team will advise of any exemptions that may apply. The use of exemptions is at the discretion of the Head of Service / member of the Senior Management Team and/or Caldicott Guardian. If the request relates to patient data the request must be copied to the GMSS Caldicott Guardian.

- **Refusing a request –** The IG team will draft a letter to respond back informing the data subject that GMSS have grounds for refusing a subject access request. Under GDPR, grounds for refusing to process a subject access request are if the request is manifestly unfounded or excessive.

- **Response** – The finalised response will be collated by the GMSS IG Team taking into account direction from the Head of Service and Caldicott Guardian. All collated information will be sent to the Head of Service and Caldicott Guardian for final approval before a written response is sent to the requestor. The final response will be sent via NHSmail to the requestor, unless the requestor has specified another method by which they wish to receive the response (e.g. post). GMSS IG Team will only provide information via channels that are secure. When hard copies of information are posted, they will be sealed securely and sent by recorded delivery.

- **Logging** – After the response has been sent to the requestor, the SAR will be considered closed and the log will be updated accordingly by the IG Team. All sent emails in personal folders are to be saved in a file on the network drive.

- **Monitoring and Reporting** – GMSS IG team will routinely monitor the requests. The Governance Committee receive monthly reports regarding the number of requests received and any issues relating to them, such as difficulty obtaining information, internal reviews and complaints. A summary is also reported to the Senior Management Team on an annual basis.

9. Accessibility

Every effort will be made to provide the requestor with information in an accessible format, especially where different formats are requested where an individual has particular communication needs associated with a disability. Requests for information in large print, translated or audio format will be considered on a case by case basis. GMSS will help individuals to understand information where possible.

The Data Protection Act / GDPR require that information is provided in an 'intelligible form'. GMSS is not required to translate information or decipher poorly handwritten notes, but best practice would be to help individuals where there are barriers to understanding the information.

If information is coded, and it is not possible for people outside of the organisation to understand to coded information, GMSS is required to provide access to the code.

10. Timescales

GMSS will respond to requests for access to information held about an individual within a month.

This is calculated from the day the request is received (whether the day after is a

working day or not) until the corresponding calendar date in the next month. For example, if a request is received on the 4th June the request must be completed by the 4th July.

There may some anomalies with this depending on how the calendar falls. For example:

- If this is not possible because the following month is shorter (and there is no corresponding calendar date) the date for a response is the last day of the following month. If the corresponding date falls on a weekend or on a public holiday you have until the next working day to respond.
- If a request is received on the 31st of a month e.g. the 31st March the time limit starts on that day. As there is no equivalent date in April the organisation have until the 30 April to comply with the request.
- If the application does not include sufficient information to identify the person making the request or to locate the information, that information should be sought promptly and the month period begins when it is supplied.

11. Complaints

If an individual or their representative is not satisfied with the outcome of their request, for example, if they feel information has been withheld or recorded incorrectly, or that they have not been allowed sufficient time to view the information, they should be informed of the options available to them to take further action.

In the first instance, the individual should be encouraged to contact the GMSS IG Team to resolve the issue locally.

An individual also has the option to escalate the matter officially to GMSS via the Caldicott Guardian or SIRO for an internal review.

An individual can escalate the matter to the ICO by using the following contact details:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 01625 545 745
e-mail: mail@ico.gsi.gov.uk

12. Training and Awareness

This policy will be made available to all staff via The Bulletin and published on GMSS Website and on People Matters for GMSS staff.

All staff are responsible for adhering to the General Data Protection Regulations 2016, Caldicott Principles, the National Data Guardian Data Security Standards, the Data Protection Act 2018 and the common law duty of confidentiality.

All staff are mandated to undertake Data Security Awareness training on an annual

basis.

Staff will receive guidance regarding this policy from a number of sources:

- Policies and procedure located on People Matters;
- Line manager;
- Other communication methods (e.g. staff briefings, team meetings, IG updates).
- The IG Team.

13. Classification of Information

GMSS implement appropriate information classifications controls, based upon the data security legislation.

Further details of the classifications controls can be found in the Information Classification Policy and the Records Management Policy.

14. Legislation & Guidelines

A set of procedural documents will be made available via People Matters.

- General Data Protection Regulations 2016
- Data Protection Act 2018
- The National Data Guardian Data Security Standards
- Confidentiality: NHS Code of Practice
- Common Law Duty of Confidence
- Human Rights Act 1998
- Computer Misuse 1998
- Electronic Communications Act 2000
- Guide to the Notification of Data Security and Protection Incidents.

15. Equality Statement

GMSS aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with the GMSS legal equality duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/belief.

The Equality Analysis has been completed and any associated policies and procedures will be analysed accordingly.

16. Monitoring and Review

This policy will be monitored through staff awareness and supporting evidence to the Data Security & Protection Toolkit.

This policy will be reviewed on a two yearly basis and in accordance with the following as and when required:

- Legislative changes;
- Good practice guidance;
- Case law;
- Significant incidents reported;
- New vulnerabilities; and
- Changes to organisational infrastructure.

The next review is scheduled for February 2022.

Appendix 1

REQUEST FOR ACCESS TO PERSONAL INFORMATION FORM

Under the Data Protection Act/GDPR, you have the right to request to any personal information we may hold about you as an organisation. This is known as a Subject Access Request. (A Subject is an individual who is the subject of personal data). Please complete this form and send back to:

Post: Information Governance – Subject Access Requests
Ellen House
Waddington St
Oldham
OL9 6EE

Email: gmss.sar@nhs.net – please ensure your write 'Subject Access Request' in the subject field of the email

1 Applicant's Full Name

……

2 Applicant's Date of Birth

……

3 Applicant's Current Address

……

……

……

4 Applicant's Previous Address (if applicable)

……

……

……

5 Applicant's Telephone Number:

Home Tel No:……

Mob Tel No:……

6 To help us search for the information you require, please tell us the about the information you require with as much detail as possible. For example, copies of personnel file between (date) and (date). If we do not receive enough information to process you request, we may be unable to process your request.

……..

……..

……..

……..

……

……

……

7 The information requested is about me?

Yes No

I confirm that I am the Data Subject

Signed:
……

Print
Name:……

Date:……..

I enclose a photocopy of 2 of the following items as proof of identity.

Please tick on the attached form which 2 forms of identity have been enclosed.

If you require information to go to a representative then please give the name and address of the representative.

Name of representative and address where information is to be sent:

……

……

……

……

8 If you require a representative to access information on your behalf then please complete the below

I give my permission
for……

to request access to my personal information as described in question 8 (below) of this form.

Signature of Data
Subject……

Print
Name:……

Name of representative and address where information is to be sent:

……

……

……

……

9. I confirm that I am the representative

Signed:……

Print Name:
……

Date:
……

We will make every effort to process your subject access request as quickly as possible within the month time limit.

However if you have any queries whilst your request is being processed, please do not hesitate to contact the IG Team at GMSS.

Appendix 2

ID Checklist

Acceptable ID documents for Subject Access Requests

To make a Subject Access Request for yourself, you will be asked to provide two forms of ID documentation, to confirm identity and address, before any information will be released.

All forms of acceptable documentation are listed in the tables below. Please note, two documents from the lists below should be provided (please send copies not originals):

Please tick against the documents you have provided.

	PROOF OF IDENTITY
	Current UK (Channel Islands, Isle of Man or Irish) passport or EU/other nationalities passports
	Passports of non-EU nationals containing UK stamps, a visa or a UK residence permit showing the immigration status of the holder in the UK *****
	Current UK (or EU/other nationalities) Photo-card Driving License (providing that the person checking is confident that non-UK Photo-card Driving Licenses are genuine
	A national ID card and/or other valid documentation relating to immigration status and permission to work*****
Any documents not listed above are not acceptable forms of identification e.g. organisational ID card.	
	Full UK Birth Certificate – issued within 6 weeks of birth
	Current Full Driving License (old version); (Provisional Driving Licenses are not acceptable)
	Residence permit issued by Home Office to EU Nationals on inspection of own-country passport
	Adoption Certificate
	Marriage/Civil Partnership certificate
	Divorce or annulment papers
	Police registration document
	Certificate of employment in HM Forces
	Current benefit book or card or original notification letter from the Department of Work and Pension (DWP) confirming legal right to benefit
	Most recent HM Revenue and Customs (previously Inland Revenue) tax notification
	Current firearms certificate
	Application Registration Card (ARC) issued to people seeking asylum in the UK (or previously issued standard acknowledgement letters, SAL1 or SAL2 forms)
	GV3 form issued to people who want to travel in the UK without valid travel documents
	Home Office letter IS KOS EX or KOS EX2
	Building industry sub-contractors certificate issued by HM Revenues and Customs (previously Inland Revenue)

	CONFIRMATION OF ADDRESS
	Recent utility bill or certificate from a supplier of utilities confirming the arrangement to pay for the services on pre-payment terms (note: mobile telephone bills should not be accepted as they can be sent to different addresses). Utility bills in joint names are permissible*****
	Local authority tax bill (valid for current year)*****
	Current UK photo-card driving license (if not already presented as a personal ID document)
	Current Full UK driving license (old version) (if not already presented as a personal ID document)
	Bank, building society or credit union statement or passbook containing current address
	Most recent mortgage statement from a recognised lender*****
	Current local council rent card or tenancy agreement
	Current benefit book or card or original notification letter from Department of Work and Pensions (DWP) confirming the rights to benefit
	Confirmation from an electoral register search that a person of that name lives at the claimed address*****
	Court Order*****

**** The date on these documents should be within the last 6 months (unless there is a good reason for it not to be e.g. clear evidence that the person was not living in the UK for 6 months or more) and they must contain the name and address of the applicant***

Appendix 3

Subject Access Request Process Flow Map