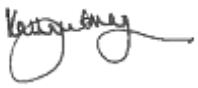
Checklist for the Review and Approval of Procedural Documents

To be completed and attached to any document which guides practices when submitted to the appropriate committee for consideration and approval.

	Yes/No/ Unsure	Comments
Title of Document		Subject Access Request Policy
Could this policy be incorporated within an existing policy?	no	
Does this policy follow the style and format of the agreed template?	yes	
Has the front sheet been completed?	yes	
Is there an appropriate review date?	yes	
Does the contents page reflect the body of the document?	yes	
Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	yes	
Are all appendices appropriate and/or applicable?	yes	
Have all appropriate stakeholders been consulted?	yes	
Has an Equality Impact Assessment been undertaken?	yes	
Is there a clear plan for implementation?	yes	
Has the document control sheet been completed?	yes	
Are key references cited and supporting documents referenced?	yes	
Does the document identify which Committee/Group will approve it?	yes	

Plans for communicating policy to – staff; practice membership; public (as appropriate)		Via the weekly news bulletin

Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name	Chief Finance Officer	Date	
Signature		09.07.19	

Committee Approval			
If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name	Chief Executive Officer	Date	09.07.19
Signature			

Subject Access Request Policy and Procedure

Version Number	V3
Ratified By	Information governance virtual group, Executive Committee
Date Ratified	IG virtual group June 2019 Executive Committee 08 July 2019
Name of Originator/Author	Information Governance Manager.
Responsible Director	Chief Finance Officer
Staff Audience	All staff
Date Issued	July 2019
Next Review Date	July 2020

DOCUMENT CONTROL

Plan Version	Page	Details of amendment	Date	Author
V1		New Policy Approved by Risk Group, sent to HR and continuing health care team for comment Feedback from HR re typo.	October 2016	RB
V2		Annual review – changes made in relation to GDPR	May 2018	IG manager
V3		Annual review Approved by IG Virtual Group and Executive Committee	May 2019	IG manager

CONTENTS

APPENDICES

1. INTRODUCTION

The General Data Protection Regulations (GDPR)/Data Protection Act 2018 (DPA 2018) 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.

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 relating to the CCG will normally be for access to view and / or to request copies of the following types of records which the CCG process. These are:

- Case files held by Continuing Health Care Team / Personalised Care Team.
- HR records and other related HR documents for CCG staff held by Human Resources with the CCG.
- Complaints / Incidents information held by the Complaints Manager, Safeguarding information held by the Safeguarding Lead for the CCG.
- Internal correspondence about a staff member/member of the public could be requested under the GDPR/Data Protections Act 2018 as a subject access request.

The CCG do not process original health records but they may hold copies of these as part of a complaint / CHC folder. If requests for health care records are made, the requester will be asked to contact the data controller which will either be the GP and / or the commissioner of the service.

2. PURPOSE

To inform staff how to deal with requests for access to information about an individual, and how HVCCG should respond to such requests. It explains the process by which patients; members of the public; staff; legal representatives and third parties can request the information.

It is important that all staff bear in mind when compiling records that the content could be requested under GDPR/ Data Protection Act 2018 as a subject access request, and to ensure that records they create are written in a way that would be appropriate to disclose.

The procedure is designed to reflect best practice in handling requests for information about an individual. Full implementation of this policy will enable the organisation to:

- Comply with legal obligations under the GDPR/Data Protection Act 2018 and the Access to Health Records Act 1990.
- Increase level of trust and confidence by being open with individuals about the information that is held about them.
- Enable individuals to verify that information held about them is accurate.

3. DEFINITIONS

Data Controller

Under GDPR/ Data Protection Act 2018, the CCG is a data controller. That is, the organisation (or person) that determines the purposes and means of the processing of personal data, and the manner in which any personal data about living individuals are processed.

Data Subject

According to the GDPR/Data Protection Act 2018, the data subject is a living individual (not an organisation) who is the subject of the personal data.

4. ROLES AND RESPONSIBILITIES

HVCCG's Information Governance Management Framework (IGMF) documents the roles and responsibilities in relation to data protection and confidentiality. This includes the role of the:

Comment [A1]: Add hyperlink

- Chief Executive Officer
- Senior Information Risk Owner (SIRO)
- Caldicott Guardian
- The Data Protection Officer
- Information Governance Manager

Virtual Information Governance Group

The Virtual IG Group are responsible for approving Information governance polices in the first instance, approval will also be sought from the Senior Leadership Team and the Executive Committee

CCG Staff are responsible for:

- Ensuring awareness of the Subject Access Request Policy and following the correct procedure as set out in this policy when receiving an access request.
- Ensuring the disclosure of information is carried out as laid down in the Subject Access Request Policy.
- Ensuring awareness of the clear guidance in place locally to report any incidents or concerns about any aspect of confidentiality and security, whether a breach has taken places or a 'near miss' has occurred using the CCG incident reporting process.

4.1 Consultation and Communication with Stakeholders

The policy has been approved by the IG Virtual Team, HR and Continuing Health Care team.

The policy will be made available to all employees of the CCG and observed by all members of staff, clinical and administrative, both temporary and permanent.

There will be an on-going professional development and educational strategy for the CCG Board, SIRO, IAO's and IAA's to accompany the implementation of this policy.

This policy will be ratified by the Information Governance Group, and Executive Committee

5. Subject Access Requests (SAR)

5.1 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 the CCG about that individual.

A SAR can be made verbally or in writing, however, the requestor does not need to mention the GDPR/Data Protection Act 2018 or 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, but their request should still be treated according to this policy. The Information Governance Manager 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 A.

A SAR can be made via any of, but not exclusively, the following methods:

- Email

- Post
- Social media
- Corporate website

SARs made online must be treated like any other SAR when they are received, however, the CCG will not provide personal information via social media channels.

5.2 Rights of access
Under GDPR/Data Protection Act 2018, any living person, who is the subject of personal information held and processed by the CCG, has a right to request access to that information. This is a legal right, subject to given exemptions below. 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 data 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.

The CCG 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. Verbal requests for information held about an individual are valid subject access requests. Identity checks will still be carried out and the CCG will provide written confirmation as to what information has been requested.

5.3 Exemptions

5.3.1 Disclosure Might Cause Harm / Third Party Information
Under the Data Protection (Subject Access Modification) Health Order 2000, the CCG has the right to deny access to all or part of records (if this applies) if one of the following condition 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 must be advised if there appears to be any grounds for withholding information.

If information has been withheld, the CCG is free to advise applicants of the grounds on which information has been withheld – but they are not obliged to do so. For example, the CCG 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.

5.3.2 Child Protection Concerns

There may be situations in which access to all or part of a child's health records can be refused – for example, where there are ongoing 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 professionals, as well as the Caldicott Guardian, before releasing any information.

5.3.3 Wishes of Deceased Patients

Health records relating to deceased people do not carry a common law duty of confidentiality. However, it is the policy of the Department of Health and the General Medical Council (GMC) that records relating to the deceased people should be treated with the same level of confidentiality as those relating to living people. For example, if the record contains a note made at the patient's request that they did not want a particular individual to know the details of their illness or their care, then no access should be granted to that individual. In addition, the record holder has the right to deny or restrict access if it felt that disclosure would cause serious harm to the physical or mental health of any other person, or would identify a third person.

If access to deceased patients records is requested this would only apply to the Continuing Health Care Team. Identity checks regarding the deceased patients legal representative / executor of will would need be satisfied to ensure the correct recipient has access / copies of any records.

5.3.4 Repeat of Earlier Request

Access to personal information can be refused where an access request has previously been granted. The GDPR/Data Protection Act 2018 permits record holders not to respond to a subsequent identical or similar request unless a reasonable interval has elapsed since the previous compliance. In determining whether a reasonable interval has elapsed, record holders should consider:

- The nature of the information
- How often it is altered
- The reason for its processing

- Whether the reason for the request(s) is also relevant

5.4 Requests from parties other than the data subject

5.4.1 Requests for Access to Records Made by a Patient Representative
Any person can authorise a representative to access information held about them on their behalf. This must be done 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, the CCG will give the individual as much assistance as possible, in order to ascertain whether consent has been granted by other means to the representative.

5.4.2 Requests for access by other organisations
Various external organisations and agencies may request information held about an individual. In almost all cases, staff must not share any information unless they have consent from the individual. Examples of requests from other agencies are listed below:

5.4.3 Solicitor
Solicitors may apply to see information held about their client, but informed, explicit and signed consent must first have been obtained from the individual before a copy of the information is released. The solicitor should be given access only to the information and explanation that would otherwise have been made available to the individual, subject to the restrictions stated above.

5.4.4 Court Order
A Court may order disclosure information (e.g. under the Civil Procedure Rules, the GDPR/Data Protection Act 2018). Unlike a request from a solicitor, a Court Order should be obeyed unless there is a robust justification to challenge it, in which case the CCG may challenge the order through the Court. The Court's decision is law, unless the CCG decides to appeal the order and take the case to a higher Court in an attempt to override the Court's decision.

Courts and Coroners are entitled to request original records. If they do, copies of the records must be retained by the CCG. Coroners normally give sufficient notice for copies to be made, but have the power to seize records at short notice, which may leave little or no time to take copies.

All Court Orders or documents appertaining to or alluding to be a Court Order

should be forwarded immediately to CCG Information Governance Manager.

5.4.5 Department of Work and Pensions

GDPR/ Data Protection Act 2018 allows (but does not require) personal data to be disclosed to assist in the assessment or collection of any tax or duty. Any request by the Department of Work and Pensions for access to any information held about an individual must be accompanied by the relevant form.

5.4.6 Police

GDPR/Data Protection Act 2018 allows (but does not require) personal data to be disclosed to assist in the prevention or detection of crime and the apprehension of prosecution of offenders.

The individual should be asked (if possible) for their informed, explicit and signed consent to disclose the information, unless this would prejudice the enquiry or court case. **Any request by the Police for access to information held about an individual must be accompanied by the relevant consent form and / or a letter detailing the information required from the Chief Superintendent of the requesting police force.**

The Crime and Disorder Act 1998 also allows (but does not require) the CCG to disclose information to the police, local authority, probation service, or health authority for the purposes of preventing crime and disorder. For the CCG to consider releasing any information without consent, the access request must relate to a serious crime in line with the Crime and Disorder Act 1998 (for example, murder or rape), otherwise the Police should be asked to obtain a Court Order or written approved signed consent (see above regarding Court Orders).

All such requests from the Police should be in writing and forwarded immediately to the Information Governance Manager.

5.4.7 Research Organisations

Although research is considered an important factor in improving healthcare, the Information Commissioner does not consider it an essential element in the provision of healthcare.

If personal identifiable information is required, informed, explicit and signed consent must be obtained. Service users are generally aware and supportive of research, but it is not reasonable to assume that they are aware of, or likely to consent to, each and every research subject or proposal.

If it is sufficient for the purposes of the research to use anonymised/ pseudonymised data, consent is not required, but patients should be informed by posters and/or leaflets how their information may be shared.

5.4.8 Parental Responsibility

Parents, or those with parental responsibility, will generally have the right to apply for access to information held about a child, although disclosure may be refused if the child is deemed competent as "Gillick competent" (see below) and refuses to give consent.

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 December 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

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

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) 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.

Where, in the view of a health professional, the child is not capable of understanding the application for access to records, the CCG 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.

5.5 Individuals living abroad
A request for access to information held about an individual made from outside the UK will be treated in the same way as a request made from within the UK. People living outside of the UK have the same rights of access to information an organisation holds about them as UK residents do.

5.6 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.

Requests for access to General Practitioner records where the patient is deceased are handled by NHS England – Primary Care Support Services. Any such application for access received by the CCG will be forwarded to NHS England – Primary Care Support Services to be processed.

NHS England – Primary Care Support Services will obtain the record from storage, copy it and send to the NHS England Area Team to be reviewed.

5.7 Third party disclosure
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).

5.8 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.

6. Subject Access Request Process

6.1 Receipt of request

Requests for information held about an individual must be made to the Information Governance Manager, Herts Valleys CCG, The Forum, Marlowes, Hemel Hempstead, Herts. HP1 1DN. The Information Governance Manager will acknowledge the request and log it on the Subject Access Request log. They will also notify the requestor of the next steps.

6.2 Confirmation of identity / further clarification and / or fees payable

If ID and clarification of a subject access request has not already been provided, the Information Governance Manager 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 for full list of ID that may be provided. ID can be photocopied and posted to the CCG or it can be scanned and emailed to the CCG.

Member of staff ID checks – the Information Governance Manager needs to check the identity of anyone making a subject access request to ensure information is only given to the person entitled to it. In the first instance, check with the member of staff's line manager that the member of staff who has submitted a request is who they say they are. If they are then you do not need to collate 2 forms of ID. Also check if there are any other circumstances which you need to be aware of pertaining to the request.

6.3 Confirmation – Once the ID /clarification have been received, the Information

Governance Manager will confirm this to the requestor and notify them that their request will be responded to within 1 calendar month . The period begins from the date that the ID/clarification is received. The requestor will be informed if there will be any deviation from the timeframe, however, such deviation should be an exception and be escalated to the Caldicott Guardian prior to informing the requestor.

6.4 Collating – The Information Governance Manager will contact and ask the relevant manager (or delegated authority within the department(s) for the required information as requested in the Subject Access Request. This may also involve an initial meeting with the relevant department to go through the request if this is required. The department who hold the information must return the required information by the deadline provided by the Information Governance Manager and / or a further meeting is arranged with the manager (or delegated person) to review and check the information. This review checks to see if there is any information which may be subject to an exemption and / or if consent is required to be collated from a third party.

The information must be reviewed / received by the given deadline to ensure the 1 month timeframe is not breached.

6.5 Response - The finalised response will be collated together with the information retrieved from the department(s) and / or a statement that the CCG does not hold the information requested or that an exemption applies. A written response will be sent back to the requestor. This will be via NHSmail, unless the requestor has specified another method by which they wish to receive the response (e.g. post). The CCG will only provide information via channels that are secure. When hard copies of information are posted, they will be sealed securely and sent by special delivery.

6.6 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 Information Governance Manager.

6.7 Monitoring and Reporting - The Information Governance Manager will routinely monitor the requests and the Senior Leadership Team will receive regular reports regarding the number of requests received and any issues relating to them, such as difficulty obtaining information, internal reviews and complaints

7. Fees

The CCG In most cases cannot charge a fee to comply with a subject access request. However, where the request is manifestly unfounded or excessive we may charge a "reasonable fee" for the administrative costs of complying with the request.
We can also charge a reasonable fee if an individual requests further copies of their

data following a request. We must base the fee on the administrative costs of providing further copies.

8. Accessibility

Every effort will be made to provide the requestor with information in an accessible format. Requests for information in large print, translated or audio format will be considered on a case by case basis, and may not necessarily be met. However, the CCG will help individuals to understand information where possible.

GDPR/The Data Protection Act 2018 requires that information is provided in an 'intelligible form'. The CCG 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 the coded information, the CCG is required to provide access to the code.

9 Timescales

The CCG will respond to requests for access to information held about an individual within 1 calendar month.

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 1 calendar month period begins when it is supplied.

10. 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 attend an informal meeting with a view to addressing and resolving the issues locally with the relevant Head of Service, Information Governance Manager

An individual also has the option to escalate the matter to the CCG Caldicott Guardian for review.

An individual can escalate the matter to the ICO 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

An individual may wish to seek legal independent advice to progress resolution of their concerns. In all cases, wherever possible, local resolution should be sought. However, the individual has the right to pursue any of these channels at any time and may wish to pursue several actions simultaneous

Monitoring Compliance

11 Outline here the arrangements for monitoring and reviewing the policy, including the person responsible and the date of review. Monitoring tools must be built into all procedural documents in order than compliance and effectiveness can be demonstrated. The approach to be adopted will depend on the policy but could include

- Audits
- Patients views and experiences
- Benchmarking
- Staff surveys
- Environmental Impact Analysis
- Complaints monitoring
- Trend Analysis
- Incident Reporting and Monitoring
- Monitoring ethnicity/diversity access

Include a description of the standards or Key Performance Indicators that are applicable to the policy.

12. EDUCATION AND TRAINING

Specific training will be provided to staff who are identified as holding information that could be subject to a subject access request. This includes the following teams:

- Continuing Health Care / Personalised Care Team
- Human Resources
- Safeguarding Lead

- Incidents / Complaints Lead

Staff belonging to these teams will be required to complete the relevant modules via the online IG Training Tool.

All staff will be made aware of subject access and the requirements of the CCG to respond within the statutory timeframe.

13. REFERENCES

GDPR/Data Protection Act 2018
Access to Health Records Act (1990)

14. ASSOCIATED DOCUMENTATION

Data Security and Protection Toolkit
NHS Digital Website
HVCCG Information Governance Policy
HVCCG Data Protection and Confidentiality Policy
HVCCG Privacy by Design Policy
HVCCG Risk Strategy and Procedure
HVCCG Information Security Policy
HVCCG Forensic Readiness Policy
NHS Information Risk Management – Good Practice Guide

Appendix A

REQUEST FOR ACCESS TO PERSONAL INFORMATION

Under the GDPR/Data Protection Act 2018, you have the right to request to any personal information we may hold about you. 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:

Information Governance Manager – Subject Access Requests
Herts Valleys CCG
The Forum
Marlowes
Hemel Hempstead
Herts. HP1 1DN

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 No: Mobile No:		
6	The information requested is about me? If **Yes**, please go to Question 8	**Yes**	**No**
7	The Applicant (whose data is being requested) must give permission for the information to be released to their representative.		

	I give my permission for *inset name* 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.
8	To help us search for the information you require and to keep costs to a minimum, 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, we may be unable to process your request.
9	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 (one to be a photographic copy). Please tick on the attached form which 2 forms of identity have been enclosed.
10	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 1 calendar month time limit.

However if you have any queries whilst your request is being processed, please do not hesitate to contact the Information Governance Manager at Herts Valleys CCG**.**

Appendix B

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, one being proof of identity and one to confirm your address, before any information will be released.

All forms of acceptable documentation are listed in the tables below. Please note, ONE document from each of the tables below should be provided (please send copies not originals): Please tick against the documents you have provided.

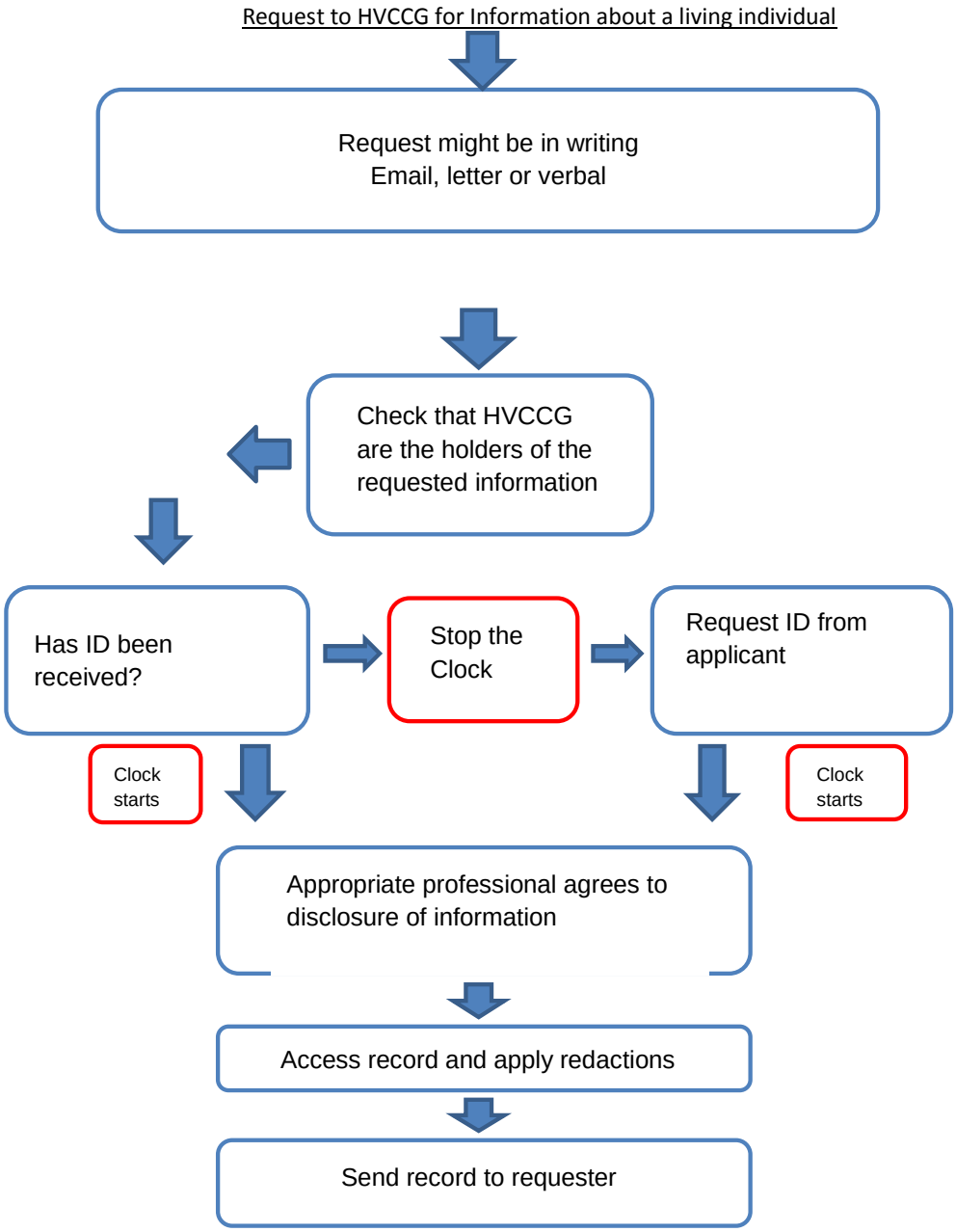
PROOF OF IDENTITY	
Acceptable Photo Personal Identity Documents	
	Current UK (Channel Islands, Isle of Man or Irish) passport or EU/other nationalities passports
	Passports of non-EU nationals containing UK stamps, a visa or a UK residence permit showing the immigration status of the holder in the UK *****
	Current UK (or EU/other nationalities) Photo-card Driving Licence (providing that the person checking is confident that non-UK Photo-card Driving Licences 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.	
Acceptable Non-Photo Personal Identity Documents	
	Full UK Birth Certificate – issued within 6 weeks of birth
	Current Full Driving Licence (old version); (Provisional Driving Licences 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	
To confirm the address, the following documents are acceptable:	
	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 licence (if not already presented as a personal ID document)
	Current Full UK driving licence (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 C

Subject Access Request – Process Map



Appendix D -

Equality Analysis - Equality Impact Assessment Screening Form

Very occasionally it will be clear that some proposals will not impact on the protected equality groups and health inequalities groups.

Where you can show that there is no impact, positive or negative, on any of the groups please complete this form and include it with any reports/papers used to make a decision on the proposal.

Name of policy / service	HVCCG Subject Access Request Policy
What is it that is being proposed?	The CCG Subject Access Request Policy aims to detail how the CCG will meet its legal obligations in relation to responding to a subject access request.
What are the intended outcome(s) of the proposal	That all CCG staff are aware of their responsibilities and are aware of legal requirements.
Explain why you think a full Equality Impact Assessment is not needed	This policy sets the information governance requirements in relation to Subject Access Requests.
On what evidence/information have you based your decision?	The policy refers to GDPR/DPA 2018 regulations
How will you monitor the impact of policy or service?	Via the Data Protection and Security Toolkit
How will you report your findings?	To the Senior Leadership Team via toolkit action plans and compliance reports
Having considered the proposal and sufficient evidence to reach a reasonable decision on actual and/or likely current and/or future impact I have decided that a full Equality Impact Assessment is not required.	
Assessors Name and Job title	Ruth Boughton Information Governance Manager

Date May 2019	