ACCESS TO PERSONAL INFORMATION

(SUBJECT ACCESS REQUEST)

POLICY

CONTENTS

EXECUTIVE SUMMARY

This policy details the requirements to be met when dealing with requests for access to health records and access to staff records as laid down by the Data Protection Act 2018 and the General Data Protection Regulations 2016, in relation to living individuals, the Access to Health Records Act 1990, specifically in relation to requests for health records of deceased individuals, and also requests for access to medical reports as laid down by the Access to Medical Reports Act 1988.

The policy provides guidance on dealing with requests for access to personal information. This includes, regardless of which team is responsible for handling the request:

- Patient Health Records
- Staff Human Resources Records
- Occupational Health Records

Director of Informatics

SCOPE AND PURPOSE

This policy applies to Stockport NHS Foundation Trust, referred to as the 'Trust', and includes all hospitals, units and community health services managed by Stockport NHS Foundation Trust.

The policy applies to all health records and all staff records, both manual & computerised, including joint records, for example health and social care records. The policy applies to all requests for such information whether originating from the data subject, solicitor, police, employee or anybody else.

Wherever, throughout the policy, the term 'record' is used this means both the manual file and the electronic record.

This policy applies to all those working in the Trust, in whatever capacity. A failure to follow the requirements of the policy may result in investigation and management action being taken as considered appropriate. This may include formal action in line with the Trust's disciplinary or capability procedures for Trust employees; and other action in relation to other workers, which may result in the termination of an assignment, placement, secondment or honorary arrangement. Non-compliance with the Policy and/or the Data Protection Act (2018) may also lead to criminal action being taken.

ROLES AND RESPONSIBILITIES

Medical Legal Team

The medico legal team is currently responsible for handling subject access requests in relation to patient's health records requested by patients and third parties on behalf of patients such as solicitors, as well as the police. They will ensure that requests for copies of patient health records

are auctioned within the appropriate timescales (see section 16) and according to the Subject Access Procedures.

The medico legal team will be required to undertake specialist training around data protection and subject access in addition to the basic Information Governance training that is provided to all staff.

Health Records Department

The health records department is currently responsible for handling all subject access requests in relation to medical reports and requests for copies of health records from other agencies such as the Department for Work and Pensions (DWP). They will ensure that requests are actioned within the appropriate timescales (see section 16) and according to the Subject Access Procedures.

The health records team will be required to undertake specialist training around data protection and subject access in addition to the basic Information Governance training that is provided to all staff.

Human Resources Department

The Human Resources department should ensure that requests for staff records are actioned within the appropriate timescales (see section 15) and according to the Subject Access Procedures. The Human Resources team will be required to undertake specialist training around data protection and subject access in addition to the basic Information Governance training that is provided to all staff.

Child Health/Radiology/Occupational Health/Estates Departments

These departments should ensure that requests for medical/identifiable information (in the case of CCTV) requests are managed in accordance with this Policy and the Subject Access Procedures (available on the IG & Security Microsite on the Trust Intranet), including the use of the Datix RFI module for recording all requests for access and should follow the time limits set out in Section 16. All staff responsible for fulfilling requests for information will be required to undertake specialist training around data protection and subject access in addition to the basic Information Governance training that is mandatory for all Trust staff.

Emergency Department

The Emergency Department should ensure that requests for information, including requests from the police are passed to the Medico-Legal department where possible, and that in cases where the information is required urgently such requests are processed in line with this policy.

Information Governance Department

The Assistant Director of Information (Governance & Security) will oversee the day-to-day management of the policy, as the Trusts Data Protection Officer. Any enquiries with regard to this policy should be directed to and dealt with by the Information Governance department.

Business Group Governance Leads

The Business Group Governance Leads may be required to review the health records in conjunction with the appropriate health professional prior to release to the patient ensuring that there is no information to be disclosed which could cause serious harm or distress to the patient (in accordance with Section 1.9 and 3).

Health Professionals

It is the responsibility of the appropriate health professional to review the health records prior to release, to determine what information, if any, should be released and what should be withheld in consideration of any serious harm or distress that may be caused to the patient

Health Professionals are responsible for effective communication with patients and providing informal access to patient records written by them where necessary and in line with section 6.3 of this policy.

Line Managers

It is the responsibility of the appropriate manager to review staff records prior to release and to decide what information, if any, should be released and what should be withheld (see section 3).

Line managers are responsible for effective communication with employees and providing informal access to staff records written by them where necessary and in line with section 3 of this policy.

Caldicott Guardian/ Chief Nurse & Dir. Of Quality

The Caldicott Guardian is a senior person responsible for safeguarding the confidentiality of patient and service-user information and enabling appropriate information-sharing. They play a key role in ensuring that the NHS, Councils with Social Services responsibilities and partner organisations satisfy the highest practicable standards for handling patient identifiable information.

The Caldicott Guardian should authorise disclosure of personal information relating to patients where the data subject has not consented to the disclosure.

Medical Director

The Medical Director has Executive responsibility for the management of health records.

Director of Human Resource

The Director of Human Resources has Executive responsibility for the management of staff records and should authorise the disclosure of personal information relating to staff where the data subject has not consented to the disclosure.

All Staff

It is the responsibility of all staff to ensure that they forward requests on to the appropriate department promptly to avoid any delay in processing the request. All staff will be required to undertake training on Information Governance including Data Protection & Subject Access. The training will be delivered via the National Learning Management System (NLMS), via the Trust's Paper Workbook or by face-to-face sessions as appropriate.

GLOSSARY OF TERMS

Data Subject

Data Subjects are the people to which the information relates. Within the workplace, they may be current employees, people applying for jobs or former employees. Data subjects might also be customers, suppliers, clients, patients, former patients, or other people information is held about.

Subject Access

Individuals whose information is held by Stockport NHS Foundation Trust have rights of access to it, regardless of the media that the information may be held/retained on. This is known as a subject access request.

Health Record

Data Protection legislation defines a health record as a record consisting of information about the physical or mental health or condition of an identifiable individual made by or on behalf of a health professional in connection with the care of that individual.

A health record can be recorded in computerised or manual form or in a mixture of both. It may include such things as; hand-written clinical notes, letters to and from other health professionals, laboratory reports, radiographs and other imaging records e.g. X-rays and not just X-ray reports, printouts from monitoring equipment, photographs, videos and tape-recordings of telephone conversations.

Employee Record

The employee record should be taken to consist of all information held regarding an individual other than that which may relate to that individual as a patient of Trust.

An employee record can be in computerised or manual form or in a mixture of both. It may include such things as; hand-written management notes, training records, occupational health records, letters to and from the employee or other members of staff, photographs, videos and, tape-recordings of telephone conversations.

Appropriate Health Professional

Under the Data Protection Act 2018 "Health Professional" means any of the following;

a) A registered medical practitioner
b) A registered dentist as defined by section 53(1) of the Dentists Act 1984,

c) A registered dispensing optician or a registered optometrist as defined by section 36(1) of the Opticians Act 1989,

d) A registered pharmacist or a registered pharmacy technician within the meaning of article 3(1) of the Pharmacy Order 2010 or a registered person as defined by Article 2(2) of the Pharmacy (Northern Ireland) Order 1976,

e) A registered nurse, midwife or health visitor,

f) A registered osteopath as defined by section 41 of the Osteopaths Act 1993

g) A registered chiropractor as defined by section 43 of the Chiropractors Act 1994,

h) A child psychotherapist

(i) A scientist employed by a health service body as head of a department.

social work professional" means any of the following—

(i) a person registered as a social worker in England in the register maintained under the Health and Social Work Professions Order 2001 (S.I. 2002/254);

(ii) a person registered as a social worker in the register maintained by Social Care Wales under section 80 of the Regulation and Inspection of Social Care (Wales) Act 2016 (anaw 2);

(iii) a person registered as a social worker in the register maintained by the Scottish Social Services Council under section 44 of the Regulation of Care (Scotland) Act 2001 (asp 8);

(iv) a person registered as a social worker in the register maintained by the Northern Ireland Social Care Council under section 3 of the Health and Personal Social Services Act (Northern Ireland) 2001 (c. 3 (N.I.)).

The '**appropriate health professional'** is defined as either;

1. "The 'health professional' who is currently or was most recently responsible for the clinical care of the data subject in connection with the information which is the subject of the request."

2. Or where there may be more than one such person, the 'appropriate health professional'' will be:

"The 'health professional' who is the most suitable to advise on the matter to which the information/subject of the request relates"

3. Or in the absence of anyone else who might qualify for the above role, the 'appropriate health professional'' will be:

"A 'health professional' who has the necessary experience and qualifications to advise on the matters to which the information/subject of the request relates"

Appropriate Manager

The **'appropriate manager'** would be a senior Human Resources manager in relation to any staff records that are held central by the Human Resources department or the employees line manager in relation to the records which they themselves hold and are responsible for.

Third Party Information

Information **from** an individual who is not the subject of the record, e.g. a relative of a patient, or a colleague, which is included in the subject's record is 'third party information'. This would include employee references or information in a child's health record from the child's parents. Similarly, information **about** a relative is 'third party information', as is any information about colleagues.

Information from a health professional who has compiled, or contributed to, the health record or has been involved in the care of the patient in his capacity as a health professional would not usually be considered third party information and should be disclosed unless serious harm to that health professional's physical or mental health or condition is likely to be caused by giving access.

Similarly, information from a manager who has compiled, or contributed to, an employee record or has been involved in the management of that employee would not usually be considered third party information.

Serious Arrestable/Indictable Offences

The Serious Organised Crime and Police Act 2005 updated the structure of police powers. The concept of arrestable and serious arrestable offences under the Police and Criminal Evidence Act 1984, which is often relied upon as the main criteria in the exercise of many police powers, were replaced by the Serious Organised Crime and Police Act 2005 with the term "indictable offence".

In order to warrant the disclosure of information offences would usually be among the most serious crimes and would generally only be tried before a jury in the Crown Court. These crimes include murder, manslaughter, rape, kidnapping, grand theft, robbery, burglary, arson, conspiracy, fraud, and other major crimes, as well as attempts to commit them.

As a guide an offence which is serious / indictable may be an offence which causes:

a) Serious harm to the state

b) Serious injury to any person
c) Serious interference
d) Death
e) Substantial financial gain
f) Serious financial loss

Further advice should be sought from the Information Governance Team and Caldicott Guardian to determine whether the offence justifies disclosure.

STEP BY STEP PROCESS

1. Requests for a Copy of the Record

1.1 Formal access to a record, or part of a record, will only be provided if it is made by any of the following:

a) The patient to which the records relate

b) An employee or previous employee to which the records relate

c) A person having parental responsibility for the data subject (where the data subject is a child under 16), **unless** it is possible to accept such a request from the child him or herself, see section 7.

d) A person appointed by the court to manage the data subject's affairs (where the data subject is incapable of managing his/her own affairs) **or** a person upon whom the data subject, when capable, has endowed a Lasting Power of Attorney.

NB: Persons with powers of attorney have no Data Protection or common law consent functions. Nevertheless, sometimes it may be appropriate to involve them as the persons who have the authority to make commercial arrangements for the data subject, including arrangements to provide both accommodation and nursing care. They, on the data subject's behalf, may have an interest in securing the best value in a nursing and care package. Where this is the case, it may be necessary to consider whether the vital interests or medical care needs of the data subject in question also require the disclosure of all or some of the sensitive personal information in question to the person who holds the power of attorney.

d) An agent acting on behalf of an intellectually capable data subject with written authority rom the data subject to make the request on their behalf. A capable person might also appoint someone to be his/her agent for the purpose of exercising data access rights by granting him/her a power of attorney, e.g. requests for data in relation to Continuing Healthcare claims, whereby a Lasting Power of Attorney for Property & Affairs, will be acceptable (see section 2.4).

e) Where the data subject has died, the data subject's personal representative and any person who may have a claim arising out of the data subject's death (see section 4).

1.2 A request for access to records in accordance with the Data Protection Act 2018 can be made either verbally or in writing, which includes by email, fax or post. However, where a request for access has been made verbally, the Trust is still required to assure itself that the applicant is legally entitled to receive the information and therefore the requirements of the section on ID checks must be followed. Although not a requirement to receive the request in writing, it will be useful if the applicant could complete the Application for Health Records form (Appendix [a]), but this cannot be enforced.

The Trust should ensure that appropriate assistance is given to serve the interest of the data subject enable that person to make a request for information. This may include advising the person that someone else may be able to help them or make the request on their behalf, or if this is not an option by offering to take a note of the applicants' details and the information that is being requested and subsequently sending the note to the applicant for confirmation

1.3 On receipt of a formal request for access to records this should be forwarded immediately to the appropriate department as defined in Section – Roles & Responsibilities. If there is not sufficient information in the formal request the relevant team may send an application form (appendix [c]/ appendix [d]) to the requestor, however the applicant is not obliged to complete the form and the relevant team may have to make such enquiries verbally.

1.4 The 'appropriate manager' should review any staff records that are being disclosed.

1.5 Where the appropriate health professional Governance Lead or appropriate manager has been asked to review a disclosure for damage & distress, they should sign a release form (appendix [a] / appendix [b]) stating they have been consulted and whether the records should be released either fully, partially or whether the request is refused.

Where both the Governance Lead and an appropriate health professional has reviewed the patients records (in the case of the potential for serious harm & distress), both the Governance Lead and the Health Professional should sign the release form.

The purpose of the release form is to evidence that the Business Group has been consulted prior to disclosing health records and that in the case of staff records, the appropriate manager has been consulted prior to the disclosure.

1.6 A request can only be refused on specific grounds.
Under the Data Protection (Subject Access Modification) (Health) Order 2000, the Trust has the right to deny a data subject access to all or part of their record if:

a) Disclosure might cause serious harm or distress

b) If, in the opinion of the appropriate health professional in charge of the patient's care, access would disclose information likely to cause serious harm to the physical or mental health or condition of the patient or any other person

c) This may include child protection concerns. There may be situations in which access to all or part of a child's record can be refused – 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

child protection professionals within the Trust, as well as the Caldicott Guardian, before releasing any information.

d) Disclosure would identify a third party

Trust policies and procedures require that all disclosures need to be reviewed to ensure that any applicable 3rd party information is redacted prior to disclosure.

- It is NOT necessary to redact the following – bearing in mind that **ALL applications are viewed on a Case by Case** basis, taking into account the individual circumstances:

- The names/details of medical staff involved in the care of the subject (ICO Code of Practice, Page 50)

- The names/details of friends/family who are present during consultations, or who evidently have a relationship with the applicant (ICO Code of Practice, Page 33)

- The names/details of 3rd parties who, it is reasonable to assume, have information in the record which is known to the applicant (ICO Code of Practice, Page 33)

  As detailed in 1.6(a) above, where the potential for damage and/or distress is clear such as in the case of disclosures involving mental health concerns, the appropriate health professional will be asked to undertake a further review of the information (in the case of healthcare records) or the appropriate Manager (in the case of staff/employee records) before the disclosure can be made.

e) Wishes of Deceased Patients

It is the policy of the Department of Health and the General Medical Council that records relating to 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 data subject'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.

f) The records are subject to legal professional privilege

g) The records are restricted by order of the courts

h) Information within the records relates to the keeping or using of gametes or embryos or pertains to an individual being born as a result of in vitro fertilisation

i) Disclosure is prohibited by law, e.g. adoption records.

Record holders must carefully consider, and be prepared to justify, any decisions to disclose or withhold information. The Caldicott Guardian must be advised if

there appear to be any grounds for withholding or restricting access to patient information. Similarly the Director of Human Resources must be advised if there appear to be any grounds for withholding or restricting access to staff information.

If information has been withheld or restricted, where possible applicants should be informed of the grounds on which information has been withheld. However the Trust is not obliged to do so and should not if this in itself could cause serious harm or distress. Details of any information withheld and the justification for doing so should be recorded alongside the record of the access request.

1.7 Where access is granted and where the information is not readily intelligible a full explanation of any abbreviations or medical terminology should be offered and thus any subsequent discussions must be documented clearly in the record.

1.8 **Documenting the request** - All requests for information must be logged on the Request for Information (RFI) module of the Datix system, ensuring that this record is fully populated. See the Subject Access Procedures for the full Datix guidance. These procedures can be found on the Information Governance & Security microsite, along with further additions such as reporting guides.

A record of all Subject Access Requests must be held in the patient's health record or employee's staff record including the Datix reference number and date provided.

1.9 **Repeat of an Earlier request** - Access to records can be refused where an access request has previously been granted. The Data Protection Act permits record holders not to respond to a subsequent identical or similar requests 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 and;
- whether the reason for the request(s) is relevant.

1.10 Wherever possible in response to a verbal request by the patient/employee, informal access should be allowed, following a review by the Business Governance Lead or the appropriate manager to the parts of the record for which they have responsibility in accordance with Section 6.3 of this policy (permitting access). Details of the disclosure should be recorded within the patient/employee record.

2. Requests to View the Record

2.1 Wherever possible in response to a verbal request by the patient/employee, informal access should be allowed, following a review by the appropriate health professional or the appropriate manager to the parts of the record for which they have responsibility in accordance with Section 6.3 of this policy (permitting access). Where the data subject wishes to view the complete record, they should complete the appropriate form shown in appendix [c] or appendix [d] and the request recorded on Datix by the department receiving the request, as appropriate.

2.2 If full or partial access is granted as decided by the appropriate health professional or the appropriate manager, the data subject should make an appointment in which they can view the record. Any decisions and access to a record should be fully documented, using the Datix RFI system.

2.3 The appropriate health professional or the appropriate manager must then decide whether the access should be supervised by themselves or whether an appointment should be made for supervision by a lay administrator e.g. ward clerk, secretary. In these circumstances the lay administrator must not comment or advise on the content of the record and if the applicant raises enquiries, an appointment with the appropriate health or the appropriate manager' should be offered. Data subjects should not be allowed to view records unsupervised in any circumstances.

2.4 The record must **not** be removed from the Trust; any requests for copies to be provided should be referred to the appropriate department and processed as a formal Subject Access Request.

2.5 Access to view records should not normally be granted to someone other than the subject of the records, at least where s/he is capable of requesting it him/herself.

3 Permitting Access

3.1 The Data Protection Act 2018 permits access to the health records and/or staff records of living individuals, whenever they were made.

3.2 The appropriate health professional, together with (where appropriate) the appropriate health professional or appropriate manager' should satisfy him/herself that providing access to the records is **not likely to cause serious harm to the physical or mental health or condition of the patient** (or any other person). [The Data Protection (Subject Access Modification) (Health) Order 2000 ('Health Order'), Article 5(1)].

3.3 **Information received from other health professionals** - Access to a record containing information relating to the patient's physical or mental health or condition cannot be denied on the grounds that the identity of a third party would be disclosed if the third party is a 'health professional' who has compiled, or contributed to, the health record or has been involved in the care of the patient in his capacity as a health professional, unless serious harm to that health professional's physical or mental health or condition is likely to be caused by giving access. The 'appropriate health professional' is responsible for permitting or denying disclosure in these cases.

Similarly access to a record containing information relating to the management of an employee cannot be denied on the grounds that the identity of a third party would be disclosed if the third party is a member of staff who has compiled or been involved in the management of that member of staff, unless serious harm to that staff member's physical or mental health or condition is likely to be caused by giving access. The 'appropriate manager' is responsible for permitting or denying disclosure in these cases.

3.4 **Joint records** - Providing access to the Trust's records is our responsibility regardless of whether the information contained within those records relates to previous care that has been provided or past employment. Requests relating to records that are shared between organisations should be processed by the organisation to which the majority of the information/subject of the request relates.

Health and Social Care Records - Access to parts of a record containing information relating to the social care of the patient cannot be denied on the grounds that the identity of a third party would be disclosed where the third party is a social worker or other social work professional unless to disclose it would cause the social worker or other social care professional serious harm.

Where the record contains information written by another organisation/body, this information should be regarded as part of the individual's record and should be treated in the same way i.e. consideration must be given to the requirements of 3rd party redaction and, where appropriate, the potential requirement to have clinical review (with regard to damage and distress to the individual e.g. child protection or Mental Health issues – see section 1.8) and therefore disclosed accordingly.

3.5 Release of Health Record information to another health professional involved in the care of the patient - It is recognised that health professionals generally need to share information amongst themselves in order to provide an effective service and care to the patient. Staff should ensure that only such information as is required for the safe management of each individual patient is disclosed and that such sharing is recorded in the patient record.

3.6 Release of staff record information to other staff members involved in the employees management - Similarly there may be circumstances in which it is necessary to provide information from an employee's staff records to other senior staff members within the organisation who are involved in an employee's management. Staff should ensure that only such information as is required is disclosed on a strict need to know basis and that such sharing is recorded in the staff record.

4 Information Relating to a Deceased Person

4.1 The Data Protection Act 2018 has superseded the Data Protection Act 1998, which itself superseded the Access to Health Records Act 1990 in relation to living individuals. However, access to health records of deceased patients is still covered by the Access to Health Records Act 1990. This Act entitles the applicant to access records made on or after 1st November 1991. Access must also be given to information recorded before this date if this is necessary to make any later part of the records intelligible.

4.2 Where the data subject has died, the data subject's personal representative is entitled to apply for access to information about the deceased. A data subject's personal representative is:

(a) An executor appointed under the deceased's will,

(b) Where there is no will, a person appointed as administrator of the deceased's estate.

4.3 If the applicant is not a Personal Representative the dependants of a deceased person may have a claim arising out of the death under the Fatal Accidents Act 1976. Dependants are defined under that Act as including:

i) The wife or husband or former wife or husband of the deceased

ii) Any person who:

a) Was living with the deceased in the same household immediately before the date of death and

b) Had been living with the deceased in the same household for at least two years before that date and

c) Was living during the whole of that period as the husband or wife of the deceased

iii. Any parent or other ascendant of the deceased

iv. Any person who was treated by the deceased as his parent

v. Any child or other descendant of the deceased (including an infant born after the death but who was en ventre sa mare (i.e. conceived but not yet born) at the time of the injury that caused the death)

vi. Any person (not being a child of the deceased) who, in the case of any marriage to which the deceased was at any time a party, was treated by the deceased as a child of the family in relation to that marriage

vii. Any person who is, or is the issue of, a brother, sister, uncle, or aunt of the deceased.

4.4 Applicants must provide proof of their entitlement to the records e.g. Where an application is being made on the basis of a claim arising from the deceased's death, applicants must provide evidence to support their claim. Once proof of appointment as a Personal Representative or that the applicant is a dependant who may have a claim arising out of the death has been obtained then it is necessary to consider which part of the records are relevant to the claim. Section 5 (4) of the Access to Health Records Act 1990 states that access shall not be given to any part of the records which, in the opinion of the holder of the records, would disclose information which is not relevant to any claim which may arise out of the data subject's death. It is necessary to consider the type of claim envisaged by the applicant and decide which records are relevant to the claim.

4.5 In addition, a claim arising out of the Inheritance (provisions for Family and Dependants) Act 1975 would also be a valid claim.

4.6 Dependants are defined under the 1975 Act as follows:

(a) A spouse or former spouse of the deceased,
(b) A child of the deceased,

(c) A child of the family,
(d) A dependant of the deceased at the time of the deceased's death.

4.7 The personal representative is the only person who has an unqualified right of access to a deceased person's record and need give no reason for applying for access to a record. Individuals other than the personal representative have a legal right of access under the Act only where they can establish a claim arising from a patient's death.

4.8 There is less clarity regarding which individuals may have a claim arising out of the patient's death. Whilst this is accepted to encompass those with a financial claim, determining who these individuals are and whether there are any other types of claim is not straightforward. The decision as to whether a claim actually exists lies with the record holder. In cases where it is not clear whether a claim arises the record holder should seek legal advice.

4.9 Before providing access to information to any personal representative of the deceased or anyone with a claim arising out of the death of the deceased, the deceased's records should be checked to ensure that the deceased made no request, when he/she was alive, that his/her records which are relevant to a legal claim arising out of the death of the deceased should not be disclosed to the applicant. In addition, the appropriate health should agree that disclosure would not be likely to cause serious harm to somebody's physical or mental health and that any third party information has been removed.

4.10 Disclosure in the absence of a statutory basis - Disclosures in the absence of a statutory basis should be in the public interest, be proportionate, and judged on a case-by-case basis. The public good that would be served by disclosure must outweigh both the obligation of confidentiality owed to the deceased individual, any other individuals referenced in a record, and the overall importance placed in the health service providing a confidential service. Key issues for consideration include any preference expressed by the deceased prior to death, the distress or detriment that any living individual might suffer following the disclosure, and any loss of privacy that might result and the impact upon the reputation of the deceased. The views of surviving family and the length of time after death are also important considerations. The obligation of confidentiality to the deceased is likely to be less than that owed to living patients and will diminish over time.

Another important consideration is the extent of the disclosure. Disclosing a complete health record is likely to require a stronger justification than a partial disclosure of information abstracted from the record. If the point of interest is the latest clinical episode or cause of death, then disclosure, where this is judged appropriate, should be limited to the pertinent details.

Individual(s) requesting access to deceased patient health information should be able to demonstrate a legitimate purpose, generally a strong public interest justification and in many cases a legitimate relationship with the deceased patient. On making a request for information, the requestor should be asked to provide authenticating details to prove their identity and their relationship with the deceased individual. They should also provide a reason for the request and where possible, specify the parts of the deceased health record they require.

Relatives, friends and carers may have a range of important reasons for requesting information about deceased patients. For example, helping a relative understand the cause

of death and actions taken to ease suffering of the patient at the time may help aid the bereavement process, or providing living relatives with genetic information about a hereditary condition may improve health outcomes for the surviving relatives of the deceased.

In some cases the decision about disclosure may not be simple or straightforward and the Caldicott Guardian or Information Governance lead, should be consulted. In the most complex cases it may be necessary to seek legal advice.

4.11 All requests for the records of deceased patients should be processed by the Medico Legal department. The applicant should complete the application form shown at appendix [c].

5. Ensuring the Identity of the Person Making the Request

In order to confirm an applicant's identity and where an applicant wishes to collect in person acceptable proof of identity will be two of the following:

a) Current passports.
b) Current Photo-card Driving Licence.
c) Utility Bill less than 6 months old

If these documents are not available a signature from a witness may be accepted where the records are being posted to a known address. An appropriate witness would be a person who has known the applicant for a minimum of three years and who is not a relative of the applicant/patient/employee.

In order to confirm an applicant's address where the applicant is the data subject and the address is different from the address on the patient or staff record, the applicant should provide a formal document or bill, which meets the following criteria:

a) Documents must be issued by a trusted source;
b) The document must be valid at the time (i.e. must be current/not more than 6 months old)
c) The document must contain the individual's name;
d) The document must contain the individual's address;
e) The document must be difficult to forge.

Examples would include the following:

- Recent utility bill or a 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
- Current Full UK driving licence (old version)
- 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;

6. Consent Requirements

6.1 Where the data subject is alive and has capacity - A data subject may request access to information about him/herself through an agent. However, the agent will enjoy no greater right of access than the data subject themselves enjoys. When applying for such access, an agent should be asked to provide written confirmation that s/he has been appointed by the data subject to exercise such rights of access to information that the data subject enjoys. (Standard application forms are attached at appendix [c] and appendix [d] depending on the nature of the information requested and a template consent form is attached at appendix [j]).

6.2 The consent should include whether all or part of the records are required and to whom they are being disclosed. In the case of partial disclosure the consent should give an indication as to which part of the record is to be disclosed e.g. incident date. The consent should be signed and dated with the last 6 months. Where the 6 months' time limit has expired, additional, up to date consent must be provided.

6.3 It is best practice to ensure that the data subject understands what information is contained within their records and what information is being disclosed so that consent can be fully informed.

6.4 **Where the data subject is incapacitated** - As the law stands, nobody is empowered to give consent on behalf of an adult. However, where a person is incapable of giving or withholding his/her consent, it will be the person in charge of that person's treatment who will decide whether information about him/her may be disclosed to someone else.

An individual may be incapable because s/he is unconscious or mentally ill, or for some other reason. In many cases, the appropriate health professional will be the person identified as the 'appropriate health professional', but this won't necessarily be the case.

Disclosure of information may only take place if it is in the data subject's 'best interests'. In order to decide whether this requirement is met, the person making the decision must consider everything that is known about the data subject (including any wishes s/he might have expressed while capable), together with the views of his/her relatives or carers. Where an adult is, or becomes, incapable of making decisions on his/her own behalf, the law provides that another may be appointed to act on his/her behalf as his/her agent.

a) **A Lasting Power of Attorney -** The Mental Capacity Act 2005 (implemented in October 2007) replaced an enduring power with the "Lasting Power of Attorney" (LPA). A person nominated under LPA can make decisions about personal welfare - which includes healthcare - as well as financial matters. An LPA must be registered with the Public Guardian to be valid. The complication here is that there can be LPA's with different roles, either for 'personal welfare' and/or 'property and affairs'. It must be clear that the LPA in question covers decisions relevant to the request i.e. personal welfare, which includes healthcare decisions, and is not restricted to another area of decision making.

b) **The Court of Protection -** Equally, the new Court of Protection - replaced the old Court of Protection in October 2007 to deal with issues of personal welfare (including healthcare) and/or 'property and affairs'. The Court of Protection can also appoint Court Deputies if a person lacking capacity needs an on-going decision maker. This can be anyone the Court feels appropriate. However, this person must be registered as a court appointed deputy.

7. Children &Young People

7.1 Where the data subject is a child (under 16), any person, with parental responsibility may apply for access to the records. Where more than one person has parental responsibility, each may independently exercise rights of access. In the case where a child lives with his or her mother and whose father applies for access to the child's records, there is no obligation to inform the child's mother that access has been sought. However, the father may only be given access to information where he has parental responsibility for the child (see 7.4). If there is doubt about whether the person applying for access or giving/withholding consent to access has parental responsibility, legal advice should be sought. **Access should only be given with the child's consent if the child is capable of understanding the request and giving his/her consent.**

7.2 Children of all ages vary in their level of maturity and understanding, and therefore, each case should be dealt with on an individual basis.

7.3 In each individual case it will be necessary to enquire of the health professional that has most recently treated the child as to whether in his/her opinion the child has reached an age where he/she has sufficient understanding and intelligence to understand the nature of the application for access to his/her records. Each application must be assessed on an individual basis.

7.4 Not all parents have parental responsibility. Both parents have parental responsibility if they were married at the time of the child's conception, or birth, or if they have jointly adopted a child. Neither parent loses parental responsibility if they divorce and this applies to both the resident and the non-resident parent. However, there are circumstances in which a father who is not married to the child's mother may acquire parental responsibility for him/her. Furthermore, parental responsibility for a child may be enjoyed by grandparents, for example, or by a local authority.

Individuals other than parents can acquire parental responsibility by an:

- **Adoption Order** – this confers full parental responsibility upon the adoptive parents and that formerly held by the birth parents is extinguished.
- **Appointment of a Guardian** (after a parent's death) – this gives guardians all the parental responsibility that the parent would have had.
- **Residence Order** – parental responsibility is shared with the parent and is subject to the limitation that the person with the order cannot withhold consent to adoption or appoint a guardian (limitation may not be relevant for the policy).
- **Parental Order** – full and permanent parental responsibility is conveyed to a married couple of a child born in surrogacy, where at least one member of the couple is the genetic parent.

According to current law, a mother always has parental responsibility for her child, save in the above circumstances. A father, however, has this responsibility only if he is married to the mother when the child is born or has acquired legal responsibility for his child through one of these three routes:

- (from 1 December 2003) by jointly registering the birth of the child with the mother

- by a parental responsibility agreement with the mother
- by a parental responsibility order, made by a court

Living with the mother, even for a long time, does not give a father parental responsibility and if the parents are not married, parental responsibility does not always pass to the natural father if the mother dies.

7.5 Where a child is "looked after" by the Local Authority permission needs to be given by both the Local Authority and the parents as they share parental responsibility.

Parental Responsibility is acquired by Local Authorities – and is shared with the parents, using the following orders:

- **Emergency Protection Order** – temporary parental responsibility is conveyed for a period of up to 8 days without prior notice to parents if necessary and can be extended by a further 7 days.
- **Interim Care Order** – temporary parental responsibility is conveyed for periods of up to 4 weeks at a time. Parental responsibility is shared with the birth parent(s). The court can issue directions regarding medical care etc.
- **Full Care Order** – parental responsibility is shared between the Local Authority and the parents, and the local authority has the power to determine the extent to which the parents can exercise their parental responsibility.

7.6 The law regards young people aged 16 to be adults for the purposes of consent to treatment and right to confidentiality. Any child, including children under the age of 16 who are judged competent to make a decision about their own medical treatment, would have the right to deny parental access to their health records. Competent young people may also seek access to their own health records.

7.7 The Data Protection Act does not allow disclosure of information whose disclosure is already prohibited in legislation concerning adoption records and reports, statements of a child's special educational needs and parental order records and reports. Health professionals who believe their records may contain such information should seek advice from the Information Governance department.

7.8 Child Protection Cases - the Children Act 2004 places certain duties on local authorities where they have reasonable cause to suspect that a child, who lives in their area, is suffering or is likely to suffer significant harm. Local authorities are required to make such enquiries, as they consider necessary to enable them to decide whether any action should be taken to promote a child's welfare.

A corresponding duty is placed upon the Trust to assist with those enquiries by providing relevant information and advice about a child if called upon to do so. If a request for information about a child is received in the context of proceedings to protect the vital interests of the child, where the consent of the child cannot be obtained, the records may be released where necessary.

Request of this nature may be accompanied by a Court Order requiring disclosure of the health records.

It is important that appropriate advice is sought via the Trust's Safeguarding Lead and Information Governance department before the records are released.

The appropriate health professional should be contacted before access to any of the information within the record is permitted.

8. Requests for Information from the Police

8.1 The Trust wishes to foster good relations with the police, and to play its part in keeping the public safe and protecting it from crime. However, the Trust also has a duty to protect the confidentiality of its patients and staff, whether they are in hospital or in the community, and whether they are alive or dead.

This duty is breached where information about a patient – **including the mere fact that she/he is a patient** – is disclosed to someone else including the police.

8.2 The Trust has a duty to comply with the provisions of the Data Protection Act 2018. It follows that information may only be disclosed with the consent of the data subject, save in exceptional circumstances.

8.3 Disclosure may be necessary and in the public interest where a failure to disclose information may expose the data subject, or others, to the risk of death or serious harm. In such circumstances the information should be disclosed promptly to an appropriate person or authority. Such circumstances may arise where the disclosure is necessary for the prevention of serious crime. The circumstances where this can arise are diverse and will need to be considered on an individual basis. They can include circumstances where a patient or former patient, employee or former employee is the victim of an offence or is suspected of having committed an offence.

8.4 Consent - If capable, an adult should be asked to give explicit consent to information about him/her being disclosed. This may not be the case when asked for information by the Police, where seeking consent may be detrimental to the investigation or prevention of a serious arrestable / indictable offence. All such requests MUST be in writing, via the Police Form provided by the relevant Police Authority. Different authorities use different versions of the form, however all forms will include the requirement that (a) the question of consent is asked and (b) that the form is counter signed by a senior Police Office, with the rank of Inspector or above. A copy of a form is attached to this document in the appendices and can be found on the Senior Manager On-Call website. All requests by the police should be authorised by the appropriate health professional/senior HR Manager, the senior manager on call or by the Caldicott Guardian before information is disclosed (see section 8.6 below).

A child of any age may also give such consent, provided s/he is sufficiently mature to understand the nature of disclosure. If the child is not sufficiently mature, consent to disclose may be given by anyone with parental responsibility of him/her (see section 7). The consent must be signed and dated within the last 6 months and must details to whom the information is being disclosed, what parts of the record are being disclosed and why the information is requested. This should be documented in the record by the member of staff processing the request.

8.5 Even if consent has been given, the procedures around permitting access still apply.

8.6 If the consent of the data subject cannot be obtained the following principles apply:

a) The police do **not** have a general right of access to records or information about patients or staff. Data Protection Act 2018 Schedule 11, paragraph 2 **allows** the disclosure of information if it is likely to assist in the apprehension/prosecution of offenders for a "serious arrestable / indictable offence" but it does not require/mandate disclosure. Unless there is a court order, the final decision about what may be disclosed will rest with the Trust. However, any request for information by the police should be considered by the relevant Business Group Governance Lead in the first instance or in relation to staff records by a senior member of staff in the Human Resources department.

b) Disclosure of confidential information may be necessary for the prevention or detection of serious crime. If, therefore, a police officer is investigating a "serious arrestable / indictable offence" the relevant Business Group Governance Lead or a senior member of the Human Resources department should bear this in mind when deciding whether or not to disclose confidential information.

c) A police officer requesting disclosure of confidential information relating to a patient or a staff member should be asked to provide:

- Confirmation that the offence being investigated is a serious arrestable / indictable offence;
- Why it is believed the subject matter of the request has committed or is about to commit such an offence;
- The reason it is believed the provision of the information requested will assist the investigation
- If the request is urgent, and the reason for this.

d) The form shown at appendix [e] should be completed by an officer not below the rank of inspector and kept by the staff member processing the request. A copy of the form should also be scanned and attached to the record of the disclosure on the Datix system.

This particular form has been developed by Greater Manchester Police (GMP) and is available to all officers in the Greater Manchester area via the GMP forms website. Other forces will have similar forms, which will require that the Officers making the request provide the same information/justification. Regardless of who handles the request, the form should be handed to the appropriate administration staff to ensure the request is logged on Datix and the outcome recorded.

e) Only information that is relevant to the police enquiry should be given. Initially this should be restricted to the name and address of the patient or member of staff, but at the discretion of the person deciding on its release, may include additional details if they are relevant to the investigation.

f) The Caldicott Guardian should be consulted prior to making any disclosures of patient personal data where consent cannot be obtained. If a decision not to disclose personal data is disputed by the police or anybody else, then this matter should be referred to the Caldicott Guardian for further consideration. The Caldicott Guardian shall consult with the

health professional in charge of the patient's treatment before a further decision is made whether or not to release the information.

g) The Director of Workforce & Organisational Development should be consulted prior to making any disclosures of staff personal data where consent cannot be obtained. If a decision not to disclose personal data is disputed by the police or anybody else then this matter should be referred to Director of Human Resources for further consideration.

h) Ensuring the request is genuine - Anyone who claims to be a police officer and to be acting as such should be asked to produce his/her warrant card. The card is credit card sized and pale blue in colour. It should include:

- The Police logo
- The officer's photo
- Their warrant number
- A signature from the chief constable

In addition, the officer should be asked for their collar number, which should match the number on the warrant card. If there is any doubt that the request is genuine verification should be sought by contacting the police (see section 21 for contact details for Greater Manchester Police).

A warrant card alone is not sufficient information to permit the disclosure of personal data, nor does it neglect the need to follow any of the procedures set out above.

Requests received over the phone should also be verified by calling back via a known switchboard.

The Subject Access Procedures contains a flowchart appendix [f] which explains in detail the process to be followed when dealing with a request from the police.

Disclosure of confidential Information without a Police Request - Situations may arise where staff become aware that a patient or member of staff may have or may be about to commit a serious arrestable / indictable offence. The police may be unaware of this but the seriousness of the offence, or for example, a threat of serious harm to another, may mean that this information should be disclosed to the police in the public interest. Staff should inform their line manager or department manager if this situation arises.

Documenting the request - A request for the disclosure of patient or staff information, and any decision to disclose such information, should be recorded on the Request for Information (RFI) module of the Datix system. Staff should ensure that this record is fully populated. A record of the disclosure should also be included in the patient's clinical records or staff employee record including the Datix reference number and data provided.

Original records should not be sent to the Police

9. Requests from Solicitors

9.1 It is preferable for requests to be made in writing, however regardless of the way a request is made, clarification of whether or not action is intended against the Trust should be obtained.

9.2 If the action against the Trust is intended a case officer in the Patient & Customer Services department should be informed immediately.

9.3 If the request is in relation to staff grievances or investigations etc. a senior member of the Human Resources Management team should be informed immediately.

9.4 If the request is in relation to childcare proceedings, a witness summons should be submitted with the application.

9.5 Written consent must be submitted with the application, and it must be current (i.e. signed and dated no more than 6 months ago).

9.6 Original records must not be sent to solicitors. If the Trust's solicitors require original records this should be authorised by the Asst. Director of Information/Data Protection Officer who will ensure that adequate security measures are taken and that a copy of the latest episode is retained where applicable.

9.7 Solicitors have no greater right of access to information than is enjoyed by their client. Where necessary and where insufficient information has been provided the application forms shown in appendix [c] or appendix [d] should be completed. The data subject's consent must also be provided. A template consent form is shown at appendix [j]. A similar consent form received from solicitors is also acceptable as long as it contains sufficient detail regarding the access request, including to whom the information is being disclosed and specifically what parts of the record should be disclosed.

10. Court Order/Affadavit

10.1 Often disclosure of personal information, and most often health records, of the alleged victim of, or witness to, a crime is requested by the alleged perpetrator's defence lawyers, and occasionally by the Crown Prosecution Service or prosecution team. Initial refusal by the Trust to release such records will usually be met by a witness summons being issued by the court (under the Criminal procedure (Attendance of Witnesses) Act 1965 in the Crown Court. The defence legal team are only entitled to have access to confidential material that is relevant to the matters in issue in the criminal trial. They are not entitled to trawl through a patients/victims entire medical history seeking material for cross-examination.

10.2 Prior to the applicant (defence/prosecution) requesting a court order to be served on the Trust they should issue the Trust with an affidavit and copy of the application notice to answer within 7 days (crown court rules 1982). This gives the Trust a period of time to decide whether the records should be disclosed or whether it would not be in the best interests of the data subject, or the third parties mentioned within the records, to disclose the whole record(s) to the court. If the data subject does not consent to disclosure, the Trust remains obliged to refuse disclosure on the grounds of confidentiality. The Trust can then either write to the court setting out the reasons why it is felt a summons should not be issued

or the Trust can attend the hearing for the summons (legal representation would be required if this is the case).

10.3 If the Trust is not issued with the affidavit, it may be served with a summons to produce the records to the court on a specific date. Failure to comply with the order may be contempt of court, and therefore a very serious matter. A Court Order will usually require a consultant/lead clinician to produce healthcare records to the court, and in these circumstances, they should not be handed over to the police, defence or prosecution.

10.4 It is essential that all records the Trust holds relating to the data subject are taken to the court. The member of staff dealing with the request should establish what records are held.

10.5 If an affidavit or court order is issued to the Trust it must immediately be telephoned through to the Deputy Director of Quality Governance or the Trust Caldicott Guardian, who can advise on the action to be taken, a copy of the affidavit/order should be sent to the appropriate person. The Information Governance department can assist with any queries.

10.6 Where information is disclosed under court order, those who disclose it will usually have a complete defence to any allegation that they have breached confidentiality, but the order must be interpreted correctly, and information only be disclosed in accordance with the terms of the order. However, even though the court has ordered production of the records the relevant Business Group Governance Lead should still review the record for anything that may harm the patient or any other person. It may then be necessary for the Trust to seek legal representation if it is felt it would not be in the best interests of the data subject, or the third parties mentioned within the records, to disclose the whole record(s) to the court. In these circumstances the Information Governance department should be contacted so that, if the Trust agrees, legal representation can be appointed.

10.7 Courts and Coroners are entitled to request original records. If they do, copies of the records must be retained by the Trust. Coroners normally give sufficient notice for copies to be made but have the power to seize records at short notice, which may leave little time to take copies. The release of records to the Coroner should be authorised by the Head / Deputy Head of Patient and Customer Services.

11. GMC/NMC/Other Investigations

It is a statutory requirement to provide this information in relation to a fitness to practice investigation and as such, consent is not required (according to GMC guidance).

There is no harm in the Trust informing the patient that we have received a request from the GMC and that we will be providing copies of their medical records, as requested, but we are not obliged to do so. The GMC themselves may inform the patient and seek consent.

The Trust Medical Director / Deputy Medical Director will be required to review the records relating to a GMC/NMC Investigation prior to disclosure, so they will be aware of the investigation as well as the potential harm that may be caused by informing the patient, so advice should be sought from the Caldicott Guardian and/or the Medical Director before informing the patient.

Where the Trust receives requests for information from organisations other than GMC/NMC

as part of an official investigation into public authority activities, for example the Police Complaints Commission, assistance should be provided in the same way that GMC/NMC investigations would be handled. All such requests must be recorded on Datix.

12. Access to Medical Reports

The Access to Medical Reports Act 1988 establishes a right of access by individuals to reports relating to themselves provided by health professionals for employment or insurance purposes.

Rights of the Patient:

Patients have the following rights:

- Their informed consent (see section 6) must be obtained before the report is dispatched.
- They may request that the completed report be retained for 21 days so that they may view the report before it is dispatched. The medical practitioner should not supply the report until this access has been given, unless 21 days have passed since the patient has communicated with the doctor about making arrangements to see the report. Access incorporates enabling the patient to attend to view the report or providing the patient with a copy of the report.
- They may request to see a copy of the report at any time within the next 6 months (so the health professional need to retain a copy for 6 months after it was written).
- They may wish to discuss the report with the health professional, and to attach a codicil if they feel that the report contains inaccuracies. However, the health professional is not obliged to alter his/her comments if there is still a difference of view (see section 19).
- They may refuse the sending of the report, so if they subsequently request access to it, the health professional must obtain their consent once again before the report is dispatched.
- Patients have a right to receive information in an **intelligible** form, and this is not necessarily in an intelligible form to the applicant. This means that it is not necessary (or a legal obligation) to translate information to another language or to have it transcribed to braille, for example, although staff should consider undertaking this taking into account the costs involved.

Rights of the Trust:

The Trust has the following rights:

- To make a **reasonable** charge for writing the report or supplying a copy of the report.
- To refuse to show the report, or a copy of the report, to the patient under the following circumstances:
  - if the report would reveal information about a third party

- if the report would reveal the identity of a third party who had given the health professional information about the patient for the report (unless that person has consented, or is a health professional).

If a patient requests access to a report, but the appropriate health professional has decided to refuse them access to part of it, it is the responsibility of the appropriate health professional to tell the patient this.

Requests for Medical Reports will be logged on the Datix system by the team handling the request and forwarded to the appropriate consultant/health professional in order for them to write the report. The consultant/health professional dealing with the request should keep the team handling the request informed of progress and the final outcome, including the date the report has been sent to allow the Datix record to be closed.

13. Requests for Information Used for Benefit Assessment Purposes (Department of Work and Pensions [DWP]) or for Benefits/Tax Fraud/Evasion

In order to assess the benefit claims of their client it is often necessary for the DWP to request sight of copies of the hospital records or to have a factual report prepared. This is in order that the claim can be objectively considered. This guidance applies also to any investigation undertaken by an appropriate statutory authority into benefits/tax fraud/evasion

13.1 The request should not be passed on to the patient's General Practitioner. If approached by the DWP for information the responsibility to provide it lies with the Trust and not a third party. The request will therefore be dealt with by the Trust and should be logged as a request, followed up, progressed and the outcome reported and closed on Datix. Any member of staff assisting with such requests must keep the handling team informed of progress and the final outcome. Any third-party information should be removed.

13.2 Consent to release of information - It is not necessary for the Trust to seek consent to release information to the DWP. The patient will be aware that the DWP may be required to make such requests and the consent from the patient is an integral part of the benefit claim form.

Schedule 2 (para 2) of the Data Protection Act 2018 also allows the disclosure of information where it is required for the assessment/collection of tax.

13.3 **Charges for release of records to the DWP** - The information required should be supplied to the DWP without charge.

13.4 Requests should be processed within 10 working days of receipt. Prompt and accurate responses are essential if the DWP are to meet their own obligations to their clients. Failure to meet the 10 day "turn round" may result in delay of benefit payment to the client, which could have a personal impact on a patient equally as much as delaying treatment.

13.5 Confidentiality - The DWP are required to handle all information in a manner that is in accordance with NHS Policy on the secure handling of confidential patient information.

14. Further Disclosures

14.1 **MP access to health information about their constituents -** The term "elected representative" covers Members of Parliament (UK, Scotland, Wales, Northern Ireland and EU), local authority councillors and mayors (and their equivalents in the devolved countries). Specific legislation under the Statutory Instrument, 2002, No. 2905, The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002 enables information to be disclosed to elected representatives without contravening the Data Protection Act 2018. However, it does not remove the constraints of the common law duty of confidentiality and as such the common law should still be satisfied (normally by consent) before information is disclosed. See the Section 13 of Model B3 in Confidentiality: NHS Code of Practice (DH 2003) for more information.

14.2 Disclosures to a Local Safeguarding Children's Board (LSCB) during the investigating a child's death - Local Safeguarding Children's Boards may require access to health records relevant to a deceased child from an NHS body to conduct an investigation/inquiry. It is highly likely that the public interest served by this process warrants full disclosure of all relevant information within the child's own records. However, in some circumstances the LSCB may also require access to information about third parties (e.g. members of the child's immediate family or carers). In all cases the LSCB should explain why it believes information about third parties is relevant to its enquiries, and you should use this to consider whether or not there is an overriding public interest to justify the disclosure of the information requested. In cases where you determine disclosure to be in the public interest you must ensure that any information you disclose about a third party is both necessary and proportionate.

14.3 Disclosures to Coroners for the purpose of carrying out an inquiry - Coroners inquiries are an important part of determining cause of death in a huge number of cases in the UK. Prompt access to confidential information regarding patients and others involved in an investigation is often vital to the reliability of the outcome of an inquiry.

It is the Department of Health's view that the public interest served by Coroners' inquiries will outweigh considerations of confidentiality unless exceptional circumstances apply.

When an NHS organisation feels that there are reasons why full disclosure is not appropriate, e.g. due to confidentiality obligations or Human Rights considerations, the following steps should be taken:

a) the Coroner should be informed about the existence of information relevant to an inquiry in all cases;
b) the concern about disclosure should be discussed with the Coroner and attempts made to reach agreement on the confidential handling of records or partial redaction of record content;
c) where agreement cannot be reached the issue will need to be considered by an administrative court.

14.4 Independent Mental Health Advocates (IMHAs) and The Mental Health Act 1983 - Under this Act, certain people ("qualifying patients") are entitled to support from an IMHA. Subject to certain conditions, section 130B of that Act says that, for the purpose of providing help to a qualifying patient, IMHAs may require the production of and inspect any records relating to the patient's detention or treatment in any hospital or to any after-care services

provided for the patient under section 117 of the Act. The Department has published guidance, which is available on the Department of Health Website, on IMHAs' rights to information which would not be disclosed in response to an access request from the qualifying patient themselves.

14.5 Disclosures in response to allegations made about the operation and conduct of staff - Where allegations are made against a NHS body in the media by patients or relatives the NHS body may wish to respond in order to maintain the reputation of the NHS. However, in doing so, the NHS body should not disclose further confidential information and the level of disclosure should be proportionate to the need, with strong considerations on the impact of possible harm caused to others.

14.6 The Caldicott Guardian or Director of Workforce & Organisational Development should authorise all disclosures of personal information where the data subject has not consented to the disclosure.

15. Research

The UK Policy Framework for Health and Social Care defines research as an attempt to derive generalisable or transferable new knowledge to answer or refine questions with scientifically sound methods. This includes studies that aim to generate hypotheses or test them, in addition to simply descriptive studies. It does not include service evaluation (designed and conducted solely to define or judge current care) or audit (designed and conducted to inform delivery of best care).

All research taking place on NHS premises, using NHS patients, staff and/or facilities must only be initiated if a NHS Research Ethics Committee (REC) and any other relevant approval body (i.e. Health Research Authority (HRA), Administration of Radioactive Substances Advisory Committee, Human Fertilisation and Embryology Authority or Medicines and Healthcare products Regulatory Agency) have favourably reviewed the research proposal and related information, where the review is expected or required. RECs in England are part of the UK Health Departments' Research Ethics Service. From a Trust perspective, the focus is on confirming the local capacity and capability of delivering the research project as aligned with HRA recommendations, which is coordinated through the Research and Innovation Office.

Caldicott Basic Principles state that "information may be passed on for a particular purpose with the patient's consent or on a "need to know" basis in certain circumstances". The "need to know" circumstances outlined include "statistical analysis and medical or health service research".

In line with HRA advice, normally only a member of the patient's existing clinical care team should have access to patient records without explicit consent in order to identify potential participants for a research project. The care team is categorised as health professionals involved in the diagnosis, treatment and care of a patient, with boundaries defined by patient expectations. However, if the research protocol specifies that a member(s) of the research team may access patient records for this purpose, with justified reason and the research protocol has received NHS REC and HRA approval, then the said member of the research team may access records in line with the protocol.

Generally, personally identifiable data is not disclosed outside the care team unless the patient has given explicit informed consent. It is a requirement of the UK Policy Framework for Health and Social Care that all research participants are afforded respect and autonomy, taking account of their capacity to understand. Where there is a difference between the research and routine practice, research participants are given information to understand the difference and make an informed choice, unless a REC agrees otherwise. Where explicit consent is sought, it is voluntary and informed and if refused or withdrawn, is done without reprisal. Fully informed consent must include information about who will have access to view patient identifiable data, arrangements to keep it secure (including if it is to be shared outside the EEA), who has the responsibility for controlling what happens with the data, what it will be used for and, how and how long it will be stored. Once informed consent has been obtained members of the research team may have full access to patient data, as outlined in the research protocol.

Disclosure of personally identifiable data outside the care team may take place for research if the data has been effectively de-personalised/ anonymised or authorised after appropriate review but this must be for public interest or to improve patient care and for medical purpose. For some studies, it may be impractical, not possible or undesirable to obtain informed consent for access to patient data. In England and Wales, personally identifiable data can be disclosed outside of the care team if it is supported under Section 251 of the NHS Act 2006. Section 251 refers explicitly to medical records and therefore does not apply to staff only studies. In these circumstances, research applications for appropriate review are considered by the HRA Confidentiality Advisory Group and a favourable opinion must be in place before members of the research team can access patient records.

The UK Policy Framework for Health and Social Care also covers the need for respect of privacy and maintaining the integrity of the care record for research purposes. All information collected for or as part of a research project must be recorded, handled and stored appropriately and in such a way and for such time that is can be accurately reported, interpreted and verified whilst patient confidentiality is upheld.

16. Time Limits

16.1 Legally, a formal request for Access to Health Records or Access to Staff Records made under Data Protection Act 2018 must be actioned and completed within 30 days from the day on which the Trust has the necessary information to confirm the identity of the applicant and locate the record.

16.2 Where the applicant has requested to view the records the Trust should offer an appointment within the 30-calendar day period. If a mutually convenient appointment cannot be agreed within this period, an alternative appointment date should be made by the end of the 30 calendar day period. The team handling the request will log it on the Datix system. The member of staff handling the request should ensure the Datix record is accurate and updated when an appointment has been made to view the records.

16.3 However, the department of Health has issued guidance that states that Trust's should be aiming to complete requests for health records within 21 days. Where possible the Trust will aim to meet this deadline.

16.4 Where an application concerns access to records or parts of records of a deceased person (made under the Access to Health Records Act 1990) that were made in the 40-day period immediately preceding the date of application, access must be given within 21 days. Where the access concerns information all of which was recorded more than 40 days before the date of application, access must be given within 30 days.

16.5 In all cases it is therefore essential that any formal request for health records is sent to the appropriate team handling the request immediately, and that any formal request for staff records are sent to the Human Resources department immediately.

16.6 Where further information/clarification has been requested but has not been received after 3 months from the date of the request, the record of the request on Datix should be closed.

17. Charges for Release of the Record

Under the Data Protection Act 2018, you cannot charge a fee to comply with a subject access request. This also applies to access to records of deceased under the Access to Health Records Act 1990

.

However, where the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

You can also charge a reasonable fee if an individual requests further copies of their data following a request. The fee must be based on the administrative costs of providing further copies. This is set out in appendix [g].

18. Sending the Record to the Applicant

18.1 All access responses should be enclosed in a sealed envelope clearly marked 'Private & Confidential - To be opened by addressee only'. Where the data subject is the applicant and the address is different to that shown on their health record or staff record, proof of identity and address (e.g. household bill or driving licence) must be obtained before the records can be sent through the post.

All mail should be directed through the Trust's post room for a return address to be marked on the reverse side of the envelope. Alternatively, the department can personally mark a **return address in case of non-delivery** on the reverse of the envelope.

Envelopes should be used which are of sufficient thickness to obscure the information contained inside. The records must be sent by tracked or registered post i.e. recorded delivery.

18.2 It would be prudent to clarify with the data subject whether they would prefer the records to be sent via post (recorded delivery) or collected in person.

19. Responses collected in Person

19.1 Where an access response is to be collected personally by the applicant, then positive proof of identity must be provided before such information is released if the applicant is unfamiliar (evidence of identity may have already been provided when the applicant made the request, see section 5, and would not need to be provided again if the evidence provided displays a photograph of the applicant, which is of a true likeness to the person collecting the records).

19.2 In order to confirm an applicant's identity and where an applicant wishes to collect in person acceptable proof of identity will be two of the following:

a) Current passports.
b) Current Photo-card Driving Licence.
c) Utility Bill less than 6 months old

If these documents are not available a signature from a witness may be accepted where the records are being posted to a known address. An appropriate witness would be a person who has known the applicant for a minimum of three years and who is not a relative of the applicant/patient/employee.

In order to confirm an applicant's address where the applicant is the data subject, and the address is different from the address on the patient or staff record. The applicant should provide a formal document or bill, which meets the following criteria:

a) Documents must be issued by a trusted source;
b) The document must be valid at the time (i.e. must be current/not more than 6 months old)
c) The document must contain the individual's name;
d) The document must contain the individual's address;
e) The document must be difficult to forge.

Examples would include the following:

- Recent utility bill or a 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
- Current Full UK driving licence (old version)
- 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;

20. What if Corrections are Requested?

20.1 Where a person considers that any information contained in the staff/patient record or part of the record to which he/she has been given access, is inaccurate, he/she may apply to the holder of the record for the necessary correction to be made (an application form is enclosed at appendix [i] or appendix [j]).

20.2 The data subject should first make an informal approach to the appropriate manager or health professional concerned to discuss the situation in an attempt to have the records amended. Where both parties agree that information is **factually** inaccurate it should be amended to clearly display the correction whilst ensuring that the original information is still legible. An explanation for the correction should also be added.

20.3 The Access to Health Records Act 1990, which applied to records put together after 1 November 1991, gave patients the legal right to have a comment added to any entry in their health record that they disagreed with. This right was lost when the Act was replaced by the Data Protection Act 1998. Under Data Protection 2018, this right has been enhanced and is termed as 'Right of Rectification', dealing with the subject's right to have inaccurate factual errors rectified. However, staff need to be mindful of the ICO guidance in this area which states that it might be possible to argue that the record of the mistake is, in itself, accurate and should be kept.

Where requests to have inaccurate personal information rectified are received, advice should be sought from the Information Governance Team.

20.4 The Trust should respond to an application to amend or remove information within 30 days, confirming compliance, or non-compliance and reasons which they believe the request is unjustified, if applicable *(see appendix [i] for employee and [j] for patient*).

21. Dealing with Complaints

21.1 If a data subject is unhappy with the outcome of their access request, for example, information was withheld from them or they feel their information has been recorded incorrectly within their record and a request to amend their record has been refused, the data subject should be encouraged to go through the following channels:

(a) The health professional or an appropriate member of the Human Resources team may wish to have an informal meeting with the individual in the hope to resolve the complaint locally.

(b) If the health professional or the Human Resources department feel that they cannot do anything for the data subject locally, the data subject should be advised to make a complaint through the Trust's complaints procedure (see the Trust's Complaint Policy for further information).

(c) Ultimately, the data subject may not wish to make a complaint through the Trust's complaints procedure and take their complaint direct to the Information Commissioner. The Information Commissioner has such powers to rule that any erroneous information is rectified, blocked, erased or destroyed and can also request an assessment around the non-disclosure of information to the applicant. Any requests for assessment from the Information Commissioner will be investigated by the Information Governance department.

(d) Alternatively, if the data subject wishes to do so, they may wish to seek legal independent advice to pursue their complaint.

IMPLEMENTATION

The responsibility of implementing this document, including training and other needs that arise shall remain with the author. Line managers have the responsibility to cascade information on new and revised policies/procedures and other relevant documents to the staff for which they manage.

Line managers must ensure that departmental systems are in place to enable staff (including agency staff) to access relevant policies, procedures, guidelines and protocols and to remain up to date with the content of new and revised policies, procedures, guidelines and protocols.

This document has been compiled by the Information Governance Team in consultation with the Patient & Customer Services Team and the Health Records Department and approved and commented on by the Governance Leads for each Business Group by means of the Information Governance & Security Group.

Once finalised, the document will be presented to the Digital Informatics Group. The document will then be displayed on the Information Governance & Security microsite on the Trust's intranet and on the Trust's website. Managers and Governance leads should ensure the information is cascaded to all staff.

This policy is directly referenced to BS 1008 and any changes to policy need to be checked for compliance.

LAUNCH AND DISSEMINATION

Launch

Safety & Risk Group
Approved by Corporate Quality Board
Intranet Office

Dissemination

Some examples of methods of disseminating information, using links to the Trust Document Microsite are as follows:

- Information cascade via relevant management teams
- Communication via Management/Departmental/Team meetings
- Inclusion of relevant information in Team Brief
- Notice board administration
- Articles in bulletins
- Briefing roadshows

MONITORING COMPLIANCE

The Trust will regularly monitor and audit its Information Governance & Security practices for compliance with this procedure.

The audit will:

- Identify areas of operation that are covered by the Trust's policies and identify which procedures and/or guidance should comply to this document;
- Follow a mechanism for adapting the procedure to cover missing areas if these are critical to processes, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the procedure is occurring and suggest a tightening of controls and adjustment to related procedures

The results of audits will be reported to the Information Governance and security, Quality Governance Committee, as appropriate.

Process for monitoring compliance with this policy

CQC Regulated Activities	Process for monitoring e.g. audit	Responsible individual/ group/ committee	Frequency of monitoring	Responsible individual/ group/ committee for review of results	Responsible individual/group/ committee for development of action plan	Responsible individual/ group/ committee for monitoring action plan and implementation
	Statistics & Data Analysis Internal Audit Information Governance Toolkit External Audit	Information Governance & Security Group	Annual	Information Governance & Security Group	Information Governance & Security Group	Information Governance & Security Group

REFERENCES AND ASSOCIATED DOCUMENTATION

References:
Information Governance Policy
Information Governance Strategy
Information Security Policy
Information Security Incident Reporting/Management

IT Acceptable Use Policy
Mobile Devices & Removable Media Security Policy
Remote Access & Mobile Working Policy
Photography/Video & Audio Records of Patients
Network Security Policy
Data Protection & Confidentiality Policy
Data Quality Policy
Freedom of Information Policy
Information Sharing and Safe Haven Policy
Records Management Policy
Records Management Strategy
Confidential Waste Policy
Disciplinary Policy
Incident Reporting SOP
BS 10008 – Evidential weight and legal admissibility of electronic information
Subject Access Procedures

EQUALITY IMPACT ASSESSMENT

Office Use Only

Submission Date:	27.11.20
Approved By:	A.HUSSAIN
Full EIA needed:	NO

Equality Impact Assessment – Policies, SOP's and Services not undergoing re-design

1	**Name of the Policy/SOP/Service**	Access to Personal Information	
2	**Department/Business Group**	Information Governance/IM&T	
3	**Details of the Person responsible for the EIA**	**Name:** **Job Title:** **Contact Details:**	Joan Carr IG Co-ordinator 0161 419 4364
4	**What are the main aims and objectives of the Policy/SOP/Service?**	This policy details the requirements to be met when dealing with requests for access to health records and access to staff records as laid down by the Data Protection Act 2018 and the General Data Protection Regulations 2016, in relation to living individuals.	

For the following question, please use the EIA Guidance document for reference:

5	**A) IMPACT** **Is the policy/SOP/Service likely to have a differential impact on any of the protected characteristics below? Please state whether it is positive or negative. What data do you have to evidence this?** **Consider:** • What does existing evidence show? E.g. consultations, demographic data, questionnaires, equality monitoring data, analysis of complaints. • Are all people from the protected characteristics equally accessing the service?	**B) MITIGATION** **Can any potential negative impact be justified? If not, how will you mitigate any negative impacts?** ✓ Think about reasonable adjustment and/or positive action ✓ Consider how you would measure and monitor the impact going forward e.g. equality monitoring data, analysis of complaints. ✓ Assign a responsible lead. ✓ Produce action plan if further data/evidence needed ✓ Re-visit after the designated time period to check for improvement.	**Lead**
Age	No Differential Impact	can be applied equally to all categories, sets out Trust policy for effective management of	

		requests	
Carers	No Differential Impact	can be applied equally to all categories, sets out Trust policy for effective management of requests	
Disability	No Differential Impact	sets out how requests can be made where the subject lacks mental capacity, applicants can request information to be provided in certain formats, ie audio, etc	
Race / Ethnicity	No Differential Impact	Applicants whose first language is not English can request information to be provided in other languages	
Gender	No Differential Impact	can be applied equally to all categories, sets out Trust policy for effective management of requests	
Gender Reassignment	No Differential Impact	can be applied equally to all categories, sets out Trust policy for effective management of requests	
Marriage & Civil Partnership	No Differential Impact	can be applied equally to all categories, sets out Trust policy for effective management of requests	
Pregnancy & Maternity	No Differential Impact	can be applied equally to all categories, sets out Trust policy for effective management of requests	
Religion & Belief	No Differential Impact	can be applied equally to all categories, sets out Trust policy for effective management of requests	
Sexual Orientation	No Differential Impact	can be applied equally to all categories, sets out Trust policy for effective management of requests	
General Comments across all equality strands	The Information Governance team will explore ways of providing requested information in formats other than in writing or by email as they arise. In addition the team will, if required, explore methods and viability of making the Trust's FOI publication scheme information available besides via the public internet site.	Applicants will need special consideration if they cannot adhere to the policy, e.g. they are homeless or do not have an email account so cannot provide an address for correspondence; do not have access to the internet so are	

	The IG team will consider options for receiving requests from applicants from disadvantaged groups, as they arise, who may not be able to provide information laid down by the law, e.g. an address for correspondence.	unaware of the request process or their rights or cannot read or write	

Action Plan

What actions have been identified to ensure equal access and fairness for all.

Action	Lead	Timescales	Review &Comments

EIA Sign-Off	**Your completed EIA should be sent to the Equality, Diversity & Inclusion Manager for approval:** equality@stockport.nhs.uk **0161 419 4784**

Quality

(Clinical and Quality Impact Assessment, Please record 'No Impact' if this is the case)

Date of Initial Review	04/01/2022
Date of Last Review	04/01/2022

Area of Impact		Consequence	Likelihood	Total	Potential Impact	Impact (Positive or Negative)	Action	Owner
Quality	Duty of Quality			0	How does it impact adversely the rights and pledges of the NHS Constitution?	No Impact		
					How does the impact affect the organisation's commitment to being an employer of choice?	No Impact		
					What is the equality impact on race, gender, age, disability, sexual orientation, religion and belief, gender reassignment, pregnancy and maternity for individuals' access to services and experience of the service?	No Impact		
	Patient Safety			0	How will this impact on the organisation's duty to protect children, young people, and adults?	No Impact		
					How will it impact on patient safety? • Infection rates • Medication errors • Significant untoward incidents and serious adverse events • Mortality & Morbidity • Failure to recognise a deteriorating	No Impact		

					patient • Safe staffing levels			
					How will it impact on preventable harm? (eg. slips, trips, falls)?	No Impact		
					How will it impact upon the reliability of safety systems? (eg. WHO checklist)	No Impact		
					How will it impact on systems and processes for ensuring that the risk of healthcare acquired infections is reduced?	No Impact		
					How will this impact on workforce capability, care and/or skills?	No Impact		
Experience	**Patient Experience**			**0**	What impact is it likely to have on self-reported experience of patients and service users? (Response to national / local surveys / complaints / PALS/incidents)	No Impact		
					How will it impact on choice?	No Impact		
					Will there be an impact on waiting times?	No Impact		
					How will it impact upon the compassionate and personalised care agenda?	No Impact		
	Staff Experience			**0**	How will it impact on recruitment of staff?	No Impact		
					What will the impact be on staff turnover and absentee rates?	No Impact		
					How will it impact on staff satisfaction surveys?	No Impact		
Effectiveness	**Clinical Effectiveness and Outcomes**			**0**	How does it impact on implementation of evidence-based practice?	No Impact		
					How will it impact on patient's length of stay?	No Impact		
					Will it reduce/impact on variations in care? (eg. readmission rates)	No Impact		
					What will the impact be upon clinical and cost-effective care delivery?	No Impact		
					How does it impact upon care pathway(s)? eg. Mortality	No Impact		
					How will it impact on target performance?	No Impact		
Other	**Please use this section to detail any other impacts to clinical and quality that are not listed in the questions.**							

Data Protection Impact Assessment

Organisations must ensure that any third parties used to process or share personal confidential data with, will ensure the data is secure and confidential and a data processing or information sharing agreement will need to be in place.

To assess the implications of using personal data, a risk assessment called a Data Protection Impact Assessment (DPIA) is required to ensure the Trust is complying with its legal obligations under the Data Protection Act 2018 and UK GDPR

If you are doing any of the following you will need to complete a Data Protection Impact Assessment (DPIA):

- Setting up a new process using personal confidential data (PCD) that identifies individuals.
- Changing an existing process which changes the way personal confidential data is used
- Procuring a new information system which holds personal confidential data

A DPIA is a proforma or risk assessment which asks questions about the process or new system based on data quality / data protection / information security and technology.

The DPIA Process:
1) Complete the screening questions below – this is to determine whether or not completion of a full DPIA is required.

2) If a full DPIA is required, you will be advised by the Information Governance Team and sent the full DPIA proforma for completion.

If DPIA's are not completed, there may be data protection concerns that have not been identified which could result in breaching the Data Protection Act/GDPR.

Advice/Guidance on completing the screening questions or the full DPIA can be provided by the Information Governance (IG) Team by emailing details of the initiative to: Information.governance@stockport.nhs.uk

DPIA Screening Questions

		Yes	No	Unsure	Comments *Document initial comments on the issue and the privacy impacts or clarification on why it is not an issue*
A)	Will the process described involve the collection of new information about individuals?		x		
B)	Does the information you are intending to process identify individuals (e.g. demographic information such as name, address, DOB, telephone, NHS number)?		x		
C)	Does the information you are intending toprocess involve sensitive information e.g.health records, criminal records or other information people would consider particularly private or raise privacy concerns?		x		
D)	Are you using information about individuals for a purpose it is not currentlyused for, or in a way it is not currently used?		x		
E)	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?		x		
F)	Will the information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		x		
G)	Does the initiative involve you using new technology which might be perceived asbeing intrusive? e.g. biometrics or facial recognition		x		
H)	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		x		
I)	Will the initiative compel individuals to provide information about themselves?		x		

1. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

If you answered YES or UNSURE to any of the above, you need to continue with the Privacy Impact Assessment. Giving false information to any of the above that subsequently results in a yes response that you knowingly entered as a NO may result in an investigation being warranted which may invoke disciplinary procedures.

DOCUMENT INFORMATION

Type of Document	Policy
Title	Access to Personal Information (Subject Access Request)
Version Number	7.1
Recommended By:	Information Governance & Security Group
Approved By:	Digital Informatics Group
Approval Date	28th September 2022
Next Review Date	September 2024
Document Author	Head of Information Governance & Security/DPO
Document Director	Director of Informatics
For use by:	All Trust employees
Specialty / Ward / Department (if local procedure document)	

CHANGE RECORD FORM

Version	Date of change	Date of release	Changed by	Reason for change
7.1	Sep 2022	Sep 2022	Joan Carr	Update of titles, added appropriate Health professional on appendix J
6.0	Oct 2020	Oct 2020	Joan Carr	Adopted the new Trust Policy Format.
5.0	Jun 2018	Jun 2018		Updating to comply with GDPR/DPA 2018 legislation
4.1	Jan 2018	Jan 2018		Further clarification on Police Requests Updating the policy to take account of GDPR requirements together with updated procedures to cover all Trust staff handling SAR

				requests
4.0	Jul 2016	Jul 2016		Refresh
3.0	Mar 2014	Mar 2014		Minor Changes to job role for Head of Patient and Customer Services.
2.1	Feb 2012	Feb 2012		Amended Serious Arrestable Offence definition to reflect indictable offense. Retained original heading to avoid confusion.
2.0	Nov 2011	Nov 2011		Adopted the new Trust Policy format. Significant Changes Made. Including inclusion of definitions; roles and responsibilities, and access requirements around human resources records.
1.3 (Final)	Sep 2009	Sep 2009		Minor Changes
1.2	Aug 2009	Aug 2009		Minor Changes
1.1	Jun 2009	Jun 2009		Minor Changes
1.0	Apr 2009	Apr 2009		New document

APPENDICES

Appendix [a] - STOCKPORT NHS FOUNDATION TRUST – HEALTH RECORD RELEASE FORM

Date:	
To (relevant Business Group Governance Lead):	
From (handler):	

Please respond by:		DH Deadline:	
		Statutory Deadline:	

Re: Access to Health Records

DP reference no:		Tracking code:	MEDLEG

Record details:

Applicant details:

The person named above has made an application to view the records detailed. I would be grateful if you could review the record and ascertain whether there is any information contained within the record that should not be disclosed to the applicant **on the grounds that it may cause serious harm to the physical or mental health or condition of the patient or of any other person.**

*Please note: the Trust **must** respond to the applicant within a **maximum of 30 days** including the records being reviewed and photocopied. Please complete the following **no later** than the response date above**.** If it is impossible to comply with this timescale please contact the Medico Legal department who may agree to extend the deadline with the applicant if there is a valid reason.*

The Caldicott Guardian should counter sign this form where the data subject's consent has not been provided to authorise the disclosure, for example police requests under section 29: Prevention/Detection of Crime.

Following review, **please complete the following** by marking the appropriate box (√). Please give details of any redactions required below.

Full access granted ☐
Partial access granted* (please give details) ☐
Access denied* (please give details) ☐

Please also ensure that the record is reviewed for **third party information** and that details of any third party information to be redacted are provided below. Information **from** a **non-health professional**, e.g. a relative of a patient, which is included in the subject's record is 'third party information'. Similarly, information **about** a relative is 'third party information'.

Checked for third party information ☐

Signed: _____

Date:

As documented in Section 6.1 of the Access to Personal Information (Subject Access) Policy, under the Data Protection (Subject Access Modification) (Health) Order 2000 (S.I. No. 413)) the information should not be provided unless the relevant Business Group Governance Lead has been consulted. The purpose behind this release form is for the Trust to have evidence that the Business Group has reviewed the disclosure and it happy to release the information.

*Please note: if access is denied rationale must be given. This will not ordinarily be conveyed to the applicant but may be required if the applicant complains against non-disclosure of the information requested either via the Trust's complaints procedure or via the Information Commissioner.

Please return completed forms to: Medico Legal Department, Patient & Customer Services, Stepping Hill Hospital.

Appendix [b] - STOCKPORT NHS FOUNDATION TRUST – STAFF RECORD RELEASE FORM

Date:	
To (appropriate manager / appropriate Gov. Lead)	
From (handler):	

Please respond by:		Statutory Deadline:	

Re: Access to Staff Records

DP reference No:	

Record details:

Applicant details:

The person named above has made an application to view the records detailed. I would be grateful if you could review the record and ascertain whether there is any information contained within the record that should not be disclosed to the applicant **on the grounds that it may cause serious harm to the physical or mental health or condition of the patient or of any other person.**

*Please note: the Trust **must** respond to the applicant within a **maximum 30 days** (legally under the General Data Protection Regulations 2018/ Data Protection Act 2018) including the records being reviewed and photocopied. Please complete the following **no later** than the response date above**.** If it is impossible to comply with this timescale please contact the Human Resources department who may agree to extend the deadline with the applicant if there is a valid reason.*

The Director of Human Resources should counter sign this form where the data subject's consent has not been provided to authorise the disclosure, for example police requests under section 29: Prevention/Detection of Crime.

Following review, please complete the following by marking the appropriate box (√). Please give details of any redactions required below.

Full access granted ☐
Partial access granted* (please give details) ☐
Access denied* (please give details) ☐

Please also ensure that the record is reviewed for **third party information** and that details of any third party information to be redacted are provided below. Information **from** a person **not involved in the management** of the employee, e.g. a colleague, which is included in the subject's record is 'third party information'. Similarly, information **about** a colleague is 'third party information'.

Checked for third party information ☐

Signed: _____

Date:

As documented in Section 6.1 of the Access to Personal Information (Subject Access) Policy the information should not be provided unless an appropriate manager or appropriate health professional where occupational health records are concerned, has been consulted. The purpose behind this release form is for the Trust to have evidence that an appropriate manager or the relevant Business Group has been consulted.

*Please note: if access is denied rationale must be given. This will not ordinarily be conveyed to the applicant but may be required if the applicant complains against non-disclosure of the information requested either via the Trust's complaints procedure or via the Information Commissioner.

Please return completed forms to: Human Resources Department, Aspen House, Stepping Hill Hospital

Appendix [c] - Application to Access Health Record Form (Patients)

Please Note:

- This form to be used for all Stockport NHS Foundation Trust records including Stockport Community Healthcare records.
- This form may be completed on-line but not submitted on-line as it requires your signature.
- Completed forms should be sent to Patient & Customer Services, Medico Legal Team, Stockport NHS Foundation Trust, Stepping Hill Hospital, Poplar Grove, Stockport, SK2 7JE. (Tel: 0161 419 5425)
- Please ensure **all** relevant documentation is attached, (if applicable) and photocopies of either (the applicant's) photocard driving licence or passport and 1 x utility bill that is no more than 6 months old and which evidences the current home address. If these documents are **not** available please contact the Medico Legal Dept. on the number above.
- Please ensure that any consent/certification is dated within the last 6 months.
- See our website (www.stockport.nhs.uk) for more details.

Patient Details:

Patients full name:			
Previous name (If applicable):			
Date of birth:	Date of death (if applicable):	Hospital unit number:	NHS number:

Most recent / last known address:	Any known previous address:

Email address (optional):			
Contact phone number:			
Date of accident (if applicable):		Date (s) of treatment:	-
Consultant / department name:			
Brief description of treatment:			
Clinic / hospital site name:			

Are x-rays required (Yes/No)?	.....
Are physiotherapy records required (Yes/No)?	.....
Disclaimer - is this in relation to a claim against Stockport NHS Foundation Trust (Yes/No)?	.....

Applicant Details:

If you are not the patient named above, please supply the following information:

Your name:	
Relationship to patient:	
Your address:	
Contact phone number:	
Email address (optional):	

Please place an (√) next to all that apply:

I am the patient	
The patient has died and I am their next of Kin.	
The patient has died and I am acting as their personal representative. I attach confirmation of my appointment.	
The patient has asked me to act for them and I attach the patient's written authorisation/consent.	
The patient is incapable of understanding the request and I attach confirmation of my appointment.	
I have parental responsibility for the patient who is under 16. He/She is incapable of understanding the request.	
I have parental responsibility for the patient who is under 16. He/She has consented to my making this request (please attach consent).	
Other (Please give details)	

Type of access request (please √):

I am applying for access to view health records	
I am applying for copies of health record	

Declaration: I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the health records referred to above under the terms of Data Protection Act 2018 / Access to Health Records Act 1990.

Checklist:
Before sending this form please check that you have completed this form in as much detail as possible & that you have:

- Signed and dated the form
- If you are acting on the patient's behalf; enclosed the patient's consent or confirmation of your or confirmation of your appointment.

Signature of **applicant:**		Print name:	
Date:		Contact telephone number:	

- Enclosed your identity documents **or** had a witness sign the certification.

View only requests:			
Official use only - Note to staff members: Please return <u>a copy</u> of this form to Patient & Customer Services, Medico Legal Department. Please do <u>not</u> detach this section of the form.			
Received / Not applicable*		**DP reference number**	
Health professional advising (Full name)		**Access provided on** (date)	
Signed:		**Date signed:**	
Further action where applicable (please (√) all that apply)			
Corrections requested:		Applicant notified of outcome:	
Copies requested / provided* (*delete as applicable): NB: Requests for copies should be directed to the Medico Legal Team.			
Comments:			

Appendix [d] - Application for Access to Staff Records

Please Note:

- This form to be used for all Stockport NHS Foundation Trust records including Stockport Community Services Staff records.
- This form may be completed on-line but not submitted on-line as it requires your signature.
- Completed forms should be sent to Human Resources, Aspen House, Stockport NHS Foundation Trust, Stepping Hill Hospital, Poplar Grove, Stockport, SK2 7JE.
- Please ensure **all** relevant documentation is attached, including consent* (if applicable) and photocopies of either the applicant's driving license or passport. If these documents are **not** available please ensure the certification is signed.
- Please ensure that any consent/certification is dated within the last 6 months.
- Contact the Human Resources Department for further details on 0161 419 5864 or visit our website (www.stockport.nhs.uk).

Staff Details:

Full name:	
Previous name (If applicable):	
Job title (s):	
Manager's name (s):	
Date of birth:	National insurance number:

Most recent / last known address:	Any known previous address:

Email address (optional):	
Contact phone number:	

Information Requested (please give details):

Personal File	
Occupational Health Record	
Training Records	
Other	

Applicant Details:

If you are not the person named above, please supply the following information:

Your name:	
Relationship to person named above:	

Your address:	
Email address (optional):	
Contact phone number:	

Please place an (√) next to all that apply:

I am an existing/past employee	
The employee**/**past employee has asked me to act for them and, and I attach their written authorisation.	
I have parental responsibility for the employee**/**past employee who is under 16. She/he is incapable of understanding the request.	
I have parental responsibility for the employee/past employee who is under 16. She/he has consented to my making this request (please attach consent where applicable).	
Other (please give details)	

Declaration: I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to staff records referred to above under the terms of Data Protection Act 2018.

Certification* (if applicable): I certify that I am (Name) of (address) and that I have known the applicant for years and have witnessed the applicant sign this form.

***This person must have known the applicant for 3+ years, or be a person of standing in the community e.g. a solicitor and must not be a relative.**

Signature of **witness:***		Print name:	
Date:		Contact telephone number:	

Checklist:

Before sending this form please check that you have completed this form in as much detail as possible and that you have:

- Signed and dated the form
- If you are acting on the staff members behalf; enclosed the staff members consent or confirmation of your appointment.
- Enclosed your identity documents **or** had a witness sign the certification.

Please Note: If there is a cost to your application this will be calculated on receipt and you will be contacted for payment before the application is processed.

1. View only requests:

2. Official use only - Note to staff members: Please return a copy of this form to Patient & Customer Services, Medico Legal Department. Please do not detach this section of the form.

	Received / Not applicable*	**DP reference number**	
Health professional advising (Full name)		**Access provided on** (date)	
Signed:		**Date signed:**	

Further action where applicable (please (√) all that apply)

Corrections requested:		Applicant notified of outcome:	
Copies requested / provided* (*delete as applicable): NB: Requests for copies should be directed to the Medico Legal Team.			

Comments:

NHS Stockport NHS Foundation Trust

Appendix [e] - Request for disclosure of personal information

This application must be authorised by an officer senior to the requesting officer and of a rank no lower than Inspector

This request for personal data is subject to the provisions of the Data Protection Act 2018, the Human Rights Act 1998 and the Common Law duty of confidentiality. It is not unlawful to process or disclose personal data in the absence of the consent of, or notification to, the data subject where the purpose is for the prevention and detection of crime or the apprehension or prosecution of offenders, and notification to the data subject would be likely to prejudice the outcome of the criminal investigation/operation. The personal data will be processed for specified purposes only, in relation to the objective of preventing or detecting crime or apprehending or prosecuting offenders,

1)

To: .....

Date: .....

The following request is required to assist in enquiries, which are concerned with and are for the purposes of:

Data Protection Act 2018 – Schedule 11 - Crime Exemption

☐ (a) the prevention or detection of crime; and / or

☐ (b) the apprehension or prosecution of offenders.

Data Protection Act 2018 – Schedule 1 Part 3 and/or Schedule 8 (3) (Vital Interests Disclosure)

☐ Information is required to protect the vital interests of the Data Subject or another person.

2) Please provide information concerning the following individual: (*sufficient detail should be provided to aid location of individual*)

Surname: ..... Other names: .....

Previous/alias name(s): .....

Gender: ..... Age: ..... DOB: .....

Present address: .....

.....

3) Information requested:

4) Brief details of why it is required (i.e. of the investigation / operation)

5) Brief details why the investigation / operation / enquiry may fail without disclosure:

I have substantial grounds for believing that failure to disclose the required information will be likely to prejudice my enquiries because:

6) Has consent been obtained / data subject notified? ☐ Yes ☐ No

Would seeking consent prejudice or compromise the investigation / enquiry? ☐ Yes ☐ No

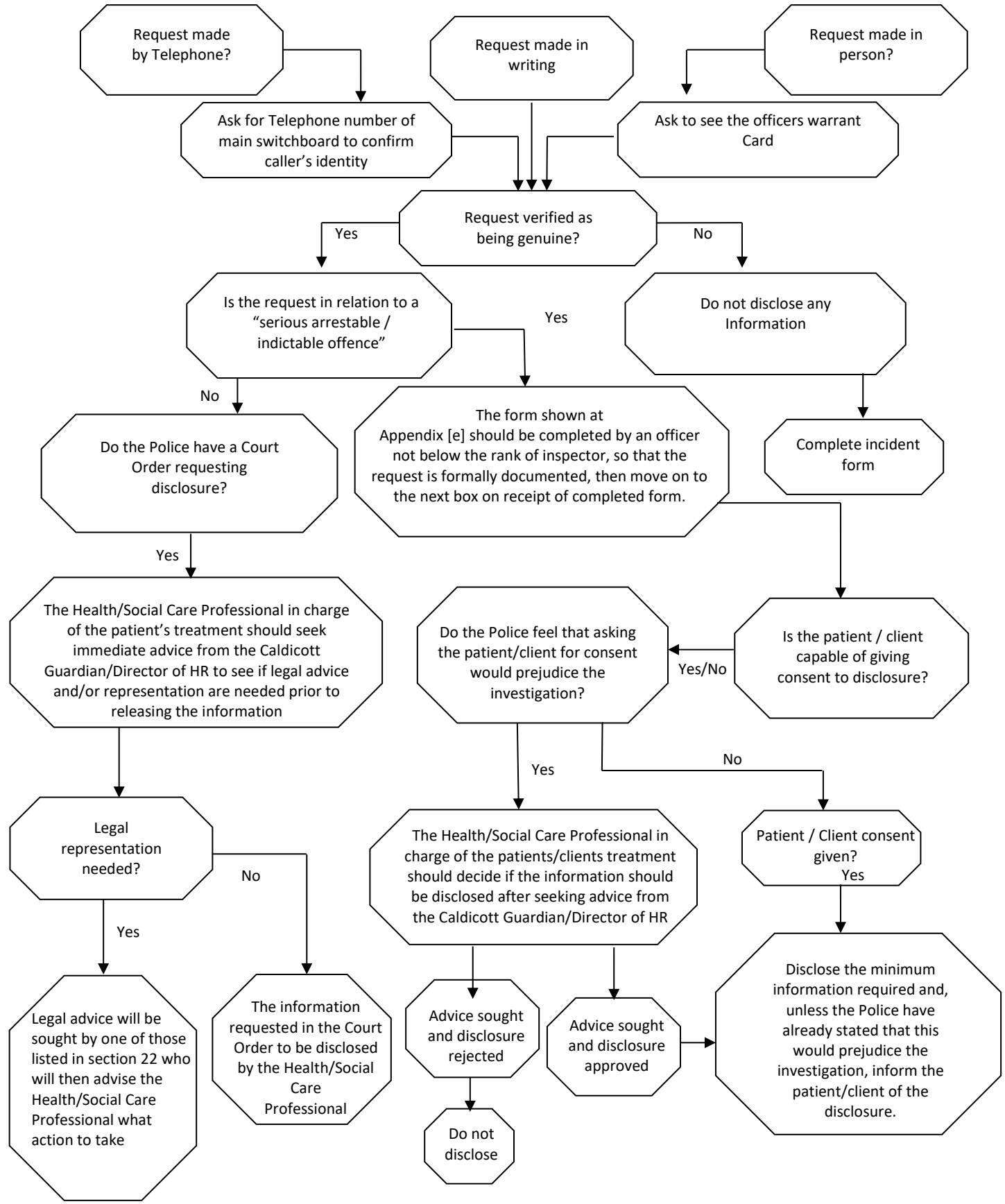
7) I confirm that:

- *the information requested will not be further processed in any manner incompatible with the stated objective;*
- *the information shall not be kept for longer than is necessary for the purposes of the stated objective;*
- *the information will be processed in accordance with the rights of the data subject under the Data Protection Act 2018;*
- *appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of and accidental loss or destruction of, or damage to, the information requested; and*
- *the details provided are, to the best of my knowledge, correct.*

I am aware of the provisions of Section 170 of the Data Protection Act 2018, regarding the unlawful obtaining of personal data.

Investigating Officer	Rank:
Signature:	Number:
Contact number:	Fax number:
Authorising Officer	Rank:
Signature:	Number:

Appendix [f] - Process for dealing with requests from the Police:



NB: All steps and decisions taken must be recorded on the RFI module of the Datix system

Appendix [g] - Request for Disclosure of Personal Information for the Purposes of a Statutory Investigation (e.g. Benefits Fraud)

NOT TO BE USED FOR DISCLOSURES TO THE POLICE

This application must be authorised by an official senior to the requesting/investigating official

This request for personal data is subject to the provisions of the Data Protection Act 2018, the Human Rights Act 1998 and the Common Law duty of confidentiality. It is not unlawful to process or disclose personal data in the absence of the consent of, or notification to, the data subject where the purpose is for the prevention and detection of crime (including tax evasion/benefit fraud) or the apprehension or prosecution of offenders, and notification to the data subject would be likely to prejudice the outcome of the criminal investigation/operation. The personal data will be processed for specified purposes only, in relation to the objective of preventing or detecting crime or apprehending or prosecuting offenders,

1)

To: .....

Date: .....

The following request is required to assist in enquiries, which are concerned with and are for the purposes of:
Data Protection Act 2018 – Schedule 2 – Part 1 (Para 2) - Crime & Taxation : General

☐ (a) the prevention or detection of crime; and / or
☐ (b) the apprehension or prosecution of offenders.
☐ (c) the assessment or collection of a tax or duty or an imposition of a similar nature

Data Protection Act 2018 – Schedule 1 Part 3 and/or Schedule 8 (3) (Vital Interests Disclosure)
☐ Information is required to protect the vital interests of the Data Subject or another person.

2) Please provide information concerning the following individual: (*sufficient detail should be provided to aid location of individual*)

Surname: ..... Other names: .....

Previous/alias name(s): .....

Gender: ..... Age: ..... DOB: .....

Present address: .....

.....

3) Information requested:

4) Brief details of why it is required (i.e. of the investigation / operation)

5) Brief details why the investigation / operation / enquiry may fail without disclosure:
I have substantial grounds for believing that failure to disclose the required information will be likely to prejudice my enquiries because:

6) Has consent been obtained / data subject notified? ☐ Yes ☐ No
Would seeking consent prejudice or compromise the investigation / enquiry? ☐ Yes ☐ No

7) I confirm that:

- *the information requested will not be further processed in any manner incompatible with the stated objective;*
- *the information shall not be kept for longer than is necessary for the purposes of the stated objective;*
- *the information will be processed in accordance with the rights of the data subject under the Data Protection Act 1998;*
- *appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of and accidental loss or destruction of, or damage to, the information requested; and*
- *the details provided are, to the best of my knowledge, correct.*

I am aware of the provisions of the Data Protection Act 2018, regarding the unlawful obtaining of personal data.

Investigating Officer Signature:	Job Title:
Contact number:	Fax number:
Authorising Officer	Job Title:

Appendix [h] – Disbursements For Repeat/Excessive Requests

Photocopying* Charges as follows (based on 10p per page):

Up to	10 Pages	£10.00
	11-20 pages	£20.00
	21-30 pages	£30.00
	31-40 copies	£40.00
	41-50 copies	£50.00
	51-60 copies	£60.00

PLUS

Postal charges will be dependent on the size and weight of the package and will correspond to Royal Mail pricing structures. Disclosures sent by Royal Mail Signed For Delivery will be charged according to Royal Mail charges and below is an extract from the current Royal Mail Pricing Guide:

UK Signed Royal Mail **Signed For®**

Size	Weight up to and including	1st Class Price	2nd Class Price
Letter	100g	£2.06	£1.95
Large Letter	100g	£2.54	£2.18
	250g	£2.94	£2.70
	500g	£3.44	£3.13
	750g	£4.25	£3.78
Small Parcel	1kg	£4.70	£4.10
	2kg	£6.57	£4.10
Medium Parcel	1kg	£6.90	£6.20
	2kg	£10.02	£6.20
	5kg	£16.85	£9.99
	10kg	£22.90	£21.25
	20kg	£33.40	£29.55
Includes compensation up to		**£50.00**	**£50.00**

Prices are exempt from VAT.

(correct as at 10th October 2020)

* All Copies Black & White and Single Sided

Appendix [i] - Application to Amend/Correct Information Contained within Employee Records

Please complete **ALL** sections of this form for any records relating to Stockport NHS Foundation Trust, including Stockport Community Healthcare records, and return to: Human Resources Department, Aspen House, Stepping Hill Hospital, Poplar Grove, Stockport, SK2 7JE

Section 1: Application Details

Employees full name:		
Previous name (if applicable):		
Job title:		
Manger's name (s):		
Date of birth	National insurance number	
Most recent / last known address:	Any known previous address:	
Telephone number:		
Email address:		

If application is being made on behalf of the data subject, state relationship to employee.

Your name:	
Relationship to employee:	
Your address:	
Telephone number:	
Email address:	

Section 2: Purpose of Request (delete as applicable)

Amendment / Correction*

**Please note: We are unable to remove information completely. If circumstances arise where information needs to be removed a line will be drawn through the selected entry and a note added stating that the information is inaccurate. This will ensure that the error does not re-occur. See section 20 of the Access to Personal Information (Subject Access) Policy for more information regarding the procedure for amending records.*

Section 3: Reason for the Request

Please state the amendments that need to be made to the record(s) and any reason(s):

Section 4: Certification

A. Employee - I certify that the information listed above is accurate and request that the amendments be made to my record.

Signed: _____ Date: _____

B: 'Appropriate Manager'

I do/do not certify that I agree to the amendments/removals* requested by the employee/employee's representative.

Signed:	
Name:	
Position:	
Date:	
Reason for non-certification (if applicable):	

Amended:	Yes/No	Date:
Removed:	Yes/No	Date:
Employee/Representative notified:	Yes/No	Date:

Appendix [j] – Application to Amend/Correct Information Contained Within Health Records

Please complete **ALL** sections of this form for any records relating to Stockport NHS Foundation Trust, including Stockport Community Healthcare records, and return to: Health Records Department, Stepping Hill Hospital, Poplar Grove, Stockport, SK2 7JE

Section 1: Application Details

Patients full name:		
Previous name (if applicable):		
Date of birth	Hospital unit number	NHS number
Most recent / last known address:	Any known previous address:	
Telephone number:		
Email address:		

If application is being made on behalf of the patient, state relationship to patient.

Your name:	
Relationship to patient:	
Your address:	
Telephone number:	
Email address:	

Section 2: Purpose of Request (delete as applicable)

Amendment / Correction*

**Please note: We are unable to remove information completely. If circumstances arise where information needs to be removed a line will be drawn through the selected entry and a note added stating that the information is inaccurate. This will ensure that the error does not re-occur. See section 20 of the Access to Personal Information (Subject Access) Policy for more information regarding the procedure for amending records.*

Section 3: Reason for the Request

Please state the amendments that need to be made to the record(s) and any reason(s):

Section 4: Certification

A. Patient - I certify that the information listed above is accurate and request that the amendments be made to my record.

Signed: _____ Date: _____

B: Appropriate Health Professional

I certify/do not certify that I agree to the amendments/removals* requested by the patient/patient's representative.

Signed:	
Name:	
Position:	
Date:	
Reason for non-certification (if applicable):	

Amended:	Yes/No	Date:
Removed:	Yes/No	Date:
Patient/Representative notified:	Yes/No	Date:

Appendix [k] - Consent Form - authority for release of personal information

IMPORTANT INFORMATION

Please ensure you have read any accompanying application notes and discussed any queries you have regarding the release of your records with your representative. Your representative should complete the form 'Application for Access to Health Records' (Reference DP02) or 'Application for Access to Staff Records' (Reference DP07).

Please ensure that you specify the periods and parts of your records you are consenting to the release of. This may include specific dates, consultant name and location, manager's name and/or parts of the records you require i.e. written diagnosis and reports.

You should also understand that failing to provide details; your representative may be entitled to access to the whole of your record history held. Subject to certain safeguards, they could be provided with details of your full history that may not be relevant for your case with your representative.

You should be aware that your representative could use your records for legal proceedings and therefore make them available to all other parties to the litigation.

To:

Department/Individual:
Stockport NHS Foundation Trust Stepping Hill Hospital Poplar Grove Hazel Grove Stockport SK2 7JE

I **name**, **date of birth**, of **address** authorise **name of representative** of **address of representative** to apply for access to my records under the Data Protection Act 1998 for records held by **Stockport NHS Foundation Trust.**

Your records will be sent to the named representative at the address specified above. Unless otherwise stated here

Signed: _____

Date: