Sheffield

Data Sharing Agreement

For

MARAC

Multi Agency Risk Assessment Conference

Revised: June 2021

Review: June 2022

Introduction

MARACs (Multi Agency Risk Assessment Conference) are multi agency meetings where all the relevant agencies share information and decide upon the most appropriate way to reduce or manage the identified risks around each case of Domestic Abuse where the victim has been assessed as being at high risk of serious harm or homicide as per the MARAC Protocol. It also applies to situations of sexual exploitation which meet the specific criteria[1] to be heard at MARAC.

The MARAC model fits into the ethos of multi –agency working, as no single agency can solve all the problems but by sharing information and working together through the MARAC process the outcomes for the victims (and their dependents) of Domestic Abuse incidents can be improved.

This MARAC Data Sharing Agreement is intended to help practitioners understand what information can be shared between the listed partners for the stated purpose(s). It also provides assurance that the partners have considered the requirements of data protection legislation.

More information can be found in the MARAC Operating Protocol.

http://sheffielddact.org.uk/domestic-abuse/resources/marac-information-and-forms/

Purpose

To identify and protect victims who have been assessed, by at least one agency or individual using the agreed risk assessment tool for domestic abuse (the DASH), as being at high risk of serious harm or homicide due to domestic abuse (or who meets the high risk criteria for adult sexual exploitation)[2]. And specifically to:

(a) Identify those victims who are of a risk of serious harm, personal harm or injury from domestic violence / sexual exploitation which is life threatening and/or traumatic and from which recovery whether physical or psychological can be expected to be difficult or impossible.
(b) Draw up a collective multi agency risk assessment
(c) Enable the most appropriate risk/reduction management plans to be drawn up.
(d) Identify the most appropriate agency/organisation to implement the tasks identified in the Action Plans
(e) Protect and safeguard the primary victim and any secondary victims, for example other household members, including children, staff/professionals working with the household, from harm

[1] Criteria as at Appendix 1
[2] Government definition plus those at risk of sexual exploitation and female genital mutilation

Organisations

- **South Yorkshire Police**, Carbrook House, 5 Carbrook Hall Road, Sheffield S9 2EH
- **Sheffield City Council**, Town Hall, 1 Pinstone Street, Sheffield S1 2HH
- **Victim Support**, Hackenthorpe Lodge, 126 Occupation Lane, Sheffield S12 4PQ
- **The Probation Service**, 45 Division Street, Sheffield, S1 4GE
- **Sheffield Futures**, 43 Division Street, Sheffield, S1 4GE
- **Sheffield Youth Justice Service,** 43 Division Street, Sheffield, S1 4GE
- **Sheffield Teaching Hospitals NHS Foundation Trust**, 8 Beech Hill Road, Sheffield, S10 2SB
- **Sheffield Children's NHS Foundation Trust,** The Mount, Glossop Road, Sheffield, S10 3FL
- **Sheffield Health and Social Care NHS Foundation Trust**, Fulwood House, 5 Old Fulwood Road, Sheffield, S10 3TG
- **IDAS**, Norfolk Chambers, 9-11 Norfolk Row, Sheffield S1 2PA
- **Shelter**, 33 – 37 Hereford Street, Sheffield, S1 4PP
- **Ashiana**, Knowle House, 4 Norfolk Park Road, Sheffield, S2 3QE
- **Sheffield Women's Aid,** PO Box 4917, Sheffield, S8 2JQ
- **Haven,** C/O The Circle, 33 Rockingham Lane, Sheffield, S1 4FW
- **Sheffield Rape and Sexual Abuse and Counselling Centre**, PO Box 34, Sheffield, S1 1UD
- **Project 6**, 646 Abbeydale Road, Sheffield, S7 2BB
- **Young Women's Housing Project,** PO Box 303 Pond Street, Sheffield, S1 1YD
- **SARC – Sexual Assault Referral Centre,** 126 Occupation Lane, Sheffield, S12 4PQ
- **Young Women's Christian Association**, Peile House, 255 Pitsmoor Road, Sheffield, S3 9AQ
- **Roundabout,** The Circle, 3 Rockingham Lane, Sheffield, S1 4FW
- **Sheffield Working Women's Opportunities Project**, 63A The Wicker, WMS House, Sheffield, S3 8HT
- **Roshni Sheffield,** 444 London Road, Sheffield, S2 4HP
- **Framework** Courtwood House, Silver Street Head, Sheffield, S1 2DD
- **Together Women Project** 106 Arundel Lane, Sheffield, S1 4RF
- **The Corner** 91 Division Street, Sheffield, S1 4GE
- **Depaul** Cumberland House, 176 Eyre Street, Sheffield, S1 4QZ
- **Cranstoun** Thames Mews, Portsmouth Mews, Esher, Surrey, Kent, KT10 9AD
- **Suzy Lamplugh** The Foundry, 17 - 19 Oval Way, London, SE11 5RR

Please note that there may also be other associated service providers. Organisations may also be added to this list due to services being contracted as contracts can change and be awarded to different organisations.

If a new organisation not listed above makes a referral to MARAC and wants to attend the conference meeting, a copy of this agreement must be sent to them at the earliest opportunity. They will be expected to sign up to this agreement either before the MARAC meeting or on attendance at the meeting.

The MARAC points of contact have overall responsibility within their respective organisations and must therefore ensure that this agreement is disseminated, understood and acted upon by the relevant practitioners.

The point of contact for each organisation will regularly monitor and review the use of this agreement to ensure that information is shared lawfully, effectively appropriately and on a 'need to know' basis.

A list of those organisations who have signed up to this agreement after the initial signing, i.e. additional organisations to the above list, will be maintained by Sheffield City Council.

Page left blank for web version

Data to be Shared

Information shared by agencies attending MARAC will be personal data, special category data and criminal offence data. It is sometimes difficult to know what is relevant and this will not always become clear until the case is discussed. Therefore, it is likely that organisations will attend MARAC with more information than they go on to share with the attending organisations because it becomes clear that information is not relevant and any sharing could be described as excessive. It is also the case that organisations may attend not planning to share information which then becomes clear is relevant to share.

The important factor for all organisations to remember is that all sharing should be relevant and proportionate and should always refer back to the purposes of the data sharing as detailed at the beginning of this agreement.

There may be circumstances, for example when a victim is at risk of serious harm or murder as a result of Honour Based Violence, where information sharing may be restricted to a small number of agencies that attend the MARAC.

It is envisaged that any data sharing will often include some or all of the following:

(a) Name, date of birth and addresses of victim

(b) Any previous name, date of birth and address of victim

(c) Name(s), date(s) of birth of victim's children or those normally resident with the victim

(d) Name and date of birth of the perpetrator

(e) Any previous name, date of birth and address of perpetrator

(f) Names(s), date(s) of birth of perpetrators children or those normally reside with the perpetrator

(g) Names and dates of birth of any other children deemed to be at risk e.g new partners children

(h) Name and dates of birth of any other adult deemed to be at risk e.g family members, new partners

(i) Information of relevant criminal convictions, court orders, injunctions, bail conditions and non-conviction information

(j) Other relevant information – this could include information relating to disability, culture, religion, General Practitioner, tenure/ property issues, debt / financial issues, vulnerabilities such as substance misuse.

(k) Weapon(s) on the premises

(l) Known children at the property

(m) Offences and allegations

It is also worth noting that audio recordings are taken at MARAC meetings. These are used for the purpose of accurate minute taking and are used most often by the minute taker only. Although these audio recordings are not proactively shared, they will be shared if requested by a partner organisation. These recordings will be securely stored electronically by the Local Authority or their designated administrator for 8 years, to ensure that we have them in the case of a Domestic Homicide Review.

Legal Considerations for sharing Information

Consent

Where consent is required for the processing and sharing of personal information as set out in the Data Protection Legislation (UK GDPR/DPA 2018) it is the responsibility of parties to seek consent to share for the purposes identified. This may only be relevant in certain situations and cases and consent could be withdrawn at any time.

It should be made clear to the data subject of the circumstances under which information will be shared with other agencies without their consent and the implications to them of not being able to share their information. The responsibility for ensuring this lies with the partner agency.

Situations where information may be shared without consent include where:

- Disclosure is in the public interest, including for the purpose of prevention or detection of crime, apprehension or prosecution of offenders
- Disclosure is to protect the vital interests of the service user
- Disclosure is enabled by legislation
- Refusing to disclose would place an adult or child at increased risk of significant harm
- Refusing to share would lead to unjustified delay in making enquiries of significant harm or serious harm

Duty of Confidentiality

This Agreement takes into account the Common Law Duty of Confidentiality which applies where information has a necessary quality of confidence or where information is imparted in circumstances giving rise to an obligation of confidence that is either explicit or implied. Where the duty applies, disclosure will be justified:

- Where the data subject has provided consent/explicit consent.

- Where disclosure is necessary to safeguard the individual, or others, or is in the public interest.
- Where there is a legal duty to do so.

Article 8 of the Human Rights Act 1998 gives people the right to a private life, family life, home and correspondence. This right means that public authorities are not allowed to interfere with a person's privacy, for example, by disclosing their personal information, unless it is lawful, necessary (in the public interest) and is for a legitimate purpose such as public safety; protection of health or morals; rights and freedoms of others and prevention of disorder or crime. In such cases the Public interest in making the disclosure must outweigh the individual's right to a private life.

Any sharing of information under this agreement will only be done where it is lawful, proportionate, relevant and necessary to do so in line with Article 8 – Human Rights Act 1998.

The Crime and Disorder Act 1998

The Crime and Disorder Act 1998 Section 115 provides a legal basis for sharing information where it is necessary for fulfilling the duties contained in the Act. The key conditions to consider under Section 115 are:

• 'relevant authorities' have the power (but not a legal duty) to share information if it is necessary for the purposes of any provision under the Crime and Disorder Act. This would include where it is necessary for the formulation and implementation of the local Crime and Disorder Reduction Strategy.

Data Protection Laws (UK GDPR and Data Protection Act 2018)

To share "personal data" as defined in the UK General Data Protection Regulation, there must be at least one lawful basis under Articles 6 and 9 (See Part 2 paragraph 10 and 18 of the Act) and processing for the 'law enforcement purposes' (see Part 3 paragraph 30 of the Act) for doing so. The lawful basis applicable to this Information Sharing and this Agreement is:

Article 6,(1)(d) "processing is necessary in order to protect the vital interests of the data subject or of another natural person"
The processing will ensure that all parties, some of whom have a legal duty, can work for the safety and well-being of those within our communities who are at high risk of serious harm or homicide.

Article 6(1)(e) " processing is necessary to perform a task in the public interest or in the exercise of official authority, and the task or function has a clear basis in law"

To share special category personal data as defined in the UK General Data Protection Regulation, there must be at least one lawful basis under Article 9 for

doing so. The lawful basis applicable to this Information Sharing and this Agreement is:

Article 9(2)(g) " Necessary for reasons of substantial public interest"

Under Data Protection Act 2018, schedule 2, Part 1 the substantial public interest conditions are:

s6 Statutory purpose

s7 Administration of justice

s8 Equality of opportunity or treatment

s10 Preventing or detecting unlawful acts

s18 Safeguarding of children and individuals at risk

Criminal Offence Data will be processed under Article 10 - Processing of personal data relating to criminal convictions and offences related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Information received from partners may be processed by South Yorkshire Police for law enforcement purposes under Data Protection Act 2018, schedule 1 Part 2 paragraph 10 and 18 and /or part 3 paragraph 30.

South Yorkshire Police has a statutory function to process personal data for any of the law enforcement purposes – prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against the prevention of threats to public security.

Any decision to disclose or share information must be necessary, justified and proportionate to risks taking into account:

- The prevention or detection of crime
- The public interest
- The right to life
- Allowing counselling, advice and support to take place

<u>Other Legal Powers</u>

There may be a requirement to share information under other legal requirements and these are set out in Appendix 3

Each organisation must ensure that information being shared is done so in line with the data protection principles, in summary:

- **Personal data shall be processed fairly, transparently and lawfully**

The majority of those referred to MARAC will be aware that this is happening because they would be present when completing the DASH form and / or will be informed by the IDVA service or another service such as the Police. Data subjects should be informed how and why their personal information will be processed and who it is shared with. However some referrals will be made without the victim's knowledge if it is unsafe to inform them as doing so would risk harm to them or others, hinder any investigation or legal proceedings.
MARAC will also have personal data regarding perpetrators, children and other possible effected parties.
"Victim's personal data and other effected parties will also be processed with reference to exemption in DPA 2018 Schedule 2 Part 1 (2), processing in order to prevent a crime. The engagement of this section exempts the processing from the first principle of fairness; therefore knowledge of the processing by the data subject is not needed.
Perpetrator's and children's personal data will also be processed under DPA 2018 Schedule 2 Part 1 (2), as above, exempting the processing from the principle of fairness".

The majority (if not all) of the information being shared between organisations as part of the MARAC process will be done so under UK GDPR Recitals 52 and 54, and Schedule 1 of the Data Protection Act 2018:

UK GDPR Recitals 52 to 54, in particular 53

> "*Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, …"*

Data Protection Act 2018

Processing of special category data can be shared when at least one condition stated in Schedule 1. For the purposes of the MARAC process these conditions will most likely be:

Part 1

(1) – Employment, social security and social protection
(2) – Health or social care purposes

Part 2 – Substantial Public Interests

18 – Safeguarding of children and of individuals at risk

19 - Safeguarding of economic well-being of certain individuals

Use of these conditions; however, requires participating organisations to comply with Schedule 1 – Part 4, parts 38-41 and have an appropriate policy document about the processing; retention schedule; storage and disposal of records.

- **Personal data is collected, for specific, explicit and legitimate purposes**

All information shared will be for the purpose detailed in this agreement. Data will not be reused for other incompatible purposes.

- **Personal Data shall be adequate, relevant and limited**

Organisations will ensure that all information shared under this agreement will be the minimum necessary required for the purpose.
The data to be shared and their relevance have been discussed between agencies at a workshop in Oct 2016. Agencies agreed that it can sometimes be difficult to know what is relevant at the beginning of a case, however all partners are committed to ensuring the continual reference to the purposes of this agreement to ensure that all information shared is adequate, relevant and limited for the purpose.

- **Personal Data shall be accurate, and where necessary, kept up to date**

Each organisation must take responsibility for ensuring that information shared is current and as up to date as possible in relation to their own contact with those being discussed. Historical information must only be shared if it is deemed to be relevant.

- **Personal data shall not be kept for longer than necessary**

The central record of MARAC minutes and information will be kept by the Local Authority or their designated administrator for 8 years in line with the duty to undertake domestic homicide reviews under Sec 9 of the Domestic Violence Crime and Victims Act 2004. Minutes should only be shared on a 'need to know' basis, securely emailed to all organisations listed after each meeting and must be password protected.
If these are not relevant to a particular organisation then they should be deleted straight away. Minutes should be stored securely in accordance with statutory guidelines and internal policies.
Agencies are informed annually of the cases that are no longer in the scope of MARAC (where no further incidents have been reported that could have constituted a crime within 12 months) so that MARAC flags can be removed from files.

- **Personal data will be processed that ensures appropriate security**

Each organisation must ensure that their IT systems are secure, that MARAC minutes are only shared with relevant staff in their organisations and that any physical security arrangements are robust.

Any sharing carried out will be done securely and all possible steps taken to prevent the unauthorised access, accidental loss or destruction, or damage to that information.
Minutes are currently securely emailed to all organisations listed after each meeting. If these are not relevant to a particular organisation then they should be deleted straight away.

A central log of all minutes will be retained by Sheffield City Council or their designated administrator so that any organisation within the ISA can refer back to minutes if necessary.

Each organisation must ensure that staff processing MARAC information are suitably trained in data protection and that data protection is included in their own processes such as staff code of conduct.

Training will also be provided during the annual MARAC induction sessions.

If a personal data breach has occurred, this must be reported to the respective organisations immediately to allow the relevant Data Protection Officer to assess and, where necessary, notify the Information Commissioner's Office within the required 72 hours.

Personal and sensitive personal information sent by email must be sent via a secure email system for public sector organisations (email systems configured in line with Government guidance, PNN, CJSM, NHS.net and N3).

Partners must note that only some public organisations have secure .gov.uk.

Partners who do not have a public sector secure email solution will be expected to utilise an acceptable encrypted email solution which can be provided by Sheffield City Council. Further details can be found at http://intranet/ict/handling-council-info/kiss/kiss-using-email/secureemails/avcosfx

Any partner concerns around the security of information must be raised immediately with Sheffield City Council who can inform any other appropriate organisations. Appropriate steps must then be taken to address those concerns.

Personal data discussed at MARAC is not expected to be transferred overseas outside of the European Union; this includes being sent or saved to the saving or distributing MARAC information or documents using online storage and file sharing facilities.
If circumstances arise where MARAC information may be transferred overseas, for example a police investigation, it must be discussed with South Yorkshire Police Performance and Governance Department and Sheffield City Council's Head of Information and Knowledge Management Team.
InformationManagement@sheffield.gov.uk

Access and Individuals' Rights

Any **Subject Access Requests**, or other requests, made by a data subject to any organisation regarding information shared at MARAC or produced by MARAC should be forwarded to both:

Sheffield City Council at SubjectAccess@sheffield.gov.uk

AND Sheffield_MARAC@southyorks.pnn.police.uk

SYP and SCC will communicate and agree SAR responses involving any other third party organisation who appear or are involved in the information being requested.

Freedom of Information Requests - public bodies which are subject to this agreement may receive FOI requests regarding MARAC.

The South Yorkshire Police contact details for FOI requests is FOI@southyorks.pnn.police.uk

Sheffield City Council contact details for FOI requests is FOI@sheffield.gov.uk

Certain data from MARAC is already published on http://www.safelives.org.uk/practice-support/resources-marac-meetings/latest-marac-data

and http://sheffielddact.org.uk/domestic-abuse/domestic-abuse-needs-analysis

Any queries regarding MARAC can be emailed to Sheffield_MARAC@southyorks.pnn.police.uk or marac@sheffield.gcsx.gov.uk

Information Governance

Datasets to be shared are the minutes of the MARAC meetings. Headline data from the minutes will also be shared at the Local MARAC Steering Group (Domestic Abuse Civil and Criminal Justice Sub Group). This group is made up of representatives of those organisations listed at the beginning of this agreement.

All information and minutes must include “Official Sensitive under the Government Secure Classification Policy”. This applies to information in any format whether physical hard copy, digital or electronic.

Data Accuracy

MARAC meetings happen approximately three times a month and so there is plenty of opportunity for any accuracy issues to be addressed. We also include the following accuracy statement in the email with minutes:

It is important that the information we record in MARAC minutes is accurate. If upon reading the minutes attached there is some inaccurate information then please contact marac@sheffield.gcsx.gov.uk

Retention and Deletion

Minutes and Audio recordings will be kept by Sheffield City Council or their designated administrator for 8 years. These will be securely stored and access will be via password protection.

Organisations who have been sent minutes which upon reading are irrelevant to them and their clients, must delete these minutes straight away.

Any information relevant to another process, for example MAPPA or Child Protection, should be transferred to the relevant records, and retained or disposed of in line with the retention policy relevant to those documents.

Organisations will retain and securely destroy information according to their own internal retention/destruction policy in line with the Data Protection legislation.

Technical and Organisational Security Arrangements

All emails will be sent via secure email, see appendix 2, which lists the email addresses to use for each organisation. This list will be maintained by the Local Authority or their designated administrator. Each organisation must keep the Local Authority or their designated administrator informed of any changes.

If secure email is not available then all information should be written in a word document which must be password protected, with the password sent on a separate email. Information about how you can do this can be found at the following link:

http://sheffielddact.org.uk/domestic-abuse/resources/marac-information-and-forms/Faxes should not be used as this is not a secure method of communication.

Any security breaches, for example, loss of data, data shared with incorrect person, data stolen, data used for other purposes (NB this list is not exhaustive) should be reported appropriately.

All organisations should follow their own security breach procedure but should also inform Sheffield City Council via InformationManagement@sheffield.gcsx.gov.uk

South Yorkshire Police via informationcompliance@southyorks.pnn.police.uk

Copying in kelly.williams@southyorks.pnn.police.uk and Gillian.Bower-Lissaman@southyorks.pnn.police.uk

And any other relevant organisations included in this sharing agreement, ie organisations who have involvement with the effected client.

Complaints

Any person wishing to make a complaint regarding MARAC should contact DACT@sheffield.gov.uk

Any complaint will be discussed between SCC and SYP who will decide between them whether either the SCC or SYP complaints policy will be followed. SCC/SYP will involve any associated organisations in the complaints process.

Review of this Agreement

This agreement will be reviewed every 12 months by SCC, SYP and at least 2 other organisations listed at the beginning of this agreement. This review should be carried out by representatives from these organisations meeting in person. Prior to the review meeting asking for feedback from all organisations involved may be required.

Termination Procedure

It is highly unlikely that MARAC will ever terminate completely, however organisations may wish to exit the sharing agreement due to contract end or organisational change. In this circumstance the organisation should inform SCC or their designated administrator as soon as possible. Even after an organisation leaves the agreement it would still be expected that the organisation would follow all retention and deletion rules as set out in this agreement. If they feel that this is not appropriate or possible they should discuss this upon leaving with SCC or their designated administrator.

Appendix 1

Sexual Exploitation Criteria

High risk refers to the high risk of the victim of serious harm and where initial interventions to reduce the risk have been unsuccessful.

High risk in the context of sexual exploitation refers to situations where the adult (18-25 years) has disclosed current sexual exploitation (but may not necessarily recognise it as this). There is evidence of sexual exploitation (e.g. police proceedings against alleged perpetrator(s). Or sexual exploitation is not confirmed but behaviours and information provided strongly suggest sexual exploitation that would cause serious harm.

Serious harm is defined as: is a risk of harm that is life threatening and / or traumatic, and from which recovery, whether physical or psychological, can be expected to be difficult or impossible. Cases will be referred where case management provision / interventions have not been successful in reducing the risk of serious harm through sexual exploitation, or where a person has not engaged with services and as a result

remains at high risk of serious harm. The referral criteria of what is high risk in Sheffield is solely based on professional judgement.

MARAC addresses specific risks, formulating an action plan to address those risks. It is proposed that the sexual exploitation service will refer cases to MARAC using a summary from Asset Plus that identifies the individual's details, specific risks and actions taken.

The sexual exploitation service will need to attend MARAC when appropriate and will represent the persons views (where known). Actions will be directed to the sexual exploitation service as appropriate.

Appendix 3

Legal Powers and Duties for Sharing

Children Act 1989	**Sections 17 and 47** place a duty on local authorities to provide services for children in need and make enquiries about any child in their area who they have reason to believe may be at risk of significant harm. Sections 17 and 47 also enable the local authority to request help from other local authorities, and NHS bodies and places an obligation on these authorities to cooperate.
Children Act 2004	**Section 10** of the Act places a duty on each children's services authority to make arrangements to promote co-operation between itself and relevant partner agencies to improve the well-being of children in their area in relation to: • Physical and mental health, and emotional well-being; • Protection from harm and neglect; • Education, training and recreation; • Making a positive contribution to society; • Social and economic well-being. Section 11 of the Act places a duty on key people and bodies to make arrangements to ensure that their functions are discharged with regard to the need to safeguard and promote the welfare of children.

Local Government Act 2000	**Section 2 (1) –** a local authority shall have the power to do anything which they consider is likely to achieve the promotion or improvement of the social wellbeing of their area
Education Act 2002	**Section 11** duty of the Children Act 2004 mirrors the duty placed by section 175 of the Education Act 2002 on LEAs and the governing bodies of both maintained schools and further education institutions to make arrangements to carry out their functions with a view to safeguarding and promoting the welfare of children and follow the guidance in Safeguarding Children in Education (DfES 2004).
Immigration and Asylum Act 1999	**Section 20 -** provides for a range of information sharing for the purposes of the Secretary of State: • to undertake the administration of immigration controls to detect or prevent criminal offences under the Immigration Act; • to undertake the provision of support for asylum seekers and their dependents.
Criminal Justice Act 2003	**Section 325 –** details the arrangements for assessing risk posed by different offenders. The "responsible authority " in relation to any area, means the chief officer of police, the local probation board and the Minister of the Crown exercising functions in relation to prisons, acting jointly. The responsible authority must establish arrangements for the purpose of assessing and managing the risks posed in that area by: • relevant sexual and violent offenders; and • other persons who, by reason of offences committed by them are considered by the responsible authority to be persons who may cause serious harm to the public (this includes children). In establishing those arrangements, the responsible authority must act in co-operation. Co-operation may include the exchange of information
The Police Act 1996	**Section 30 - (1)** gives constables all the powers and privileges of a constable throughout England and Wales and **Section 30(5)** defines these powers as powers under the enactment whenever passed or made. These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order.
Mental Capacity Act 2005	Legislation that complements the framework relating to persons who lack capacity, particularly where decision-making needs to be made on their behalf, both where mental capacity has been lost and where the incapacitating condition has been present since birth.
Caldicott Principles	These principles apply to the use of confidential information within health and social care organisations and when such information is shared with other organisations and between individuals, both for individual care and for other purposes. The principles are intended to apply to all data collected for the provision of health and social care services where patients and service users can be identified and would expect that it will be kept private. This may include for instance, details about symptoms, diagnosis, treatment, names and addresses. In some instances, the principles should also be applied to the processing of staff information.

	They are primarily intended to guide organisations and their staff, but it should be remembered that patients, service users and/or their representatives should be included as active partners in the use of confidential information. **Principle 1: Justify the purpose(s) for using confidential information** Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian. **Principle 2: Use confidential information only when it is necessary** Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible. **Principle 3: Use the minimum necessary confidential information** Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function. **Principle 4: Access to confidential information should be on a strict need-to-know basis** Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes. **Principle 5: Everyone with access to confidential information should be aware of their responsibilities** Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users. **Principle 6: Comply with the law** Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law. **Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality** Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies. **Principle 8: Inform patients and service users about how their confidential information is used** A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.
