Data Sharing Agreement: People affected by an emergency

Contents

1. Introduction to the Data Sharing Agreement

The London Resilience Forum (LRF) sets the strategy for the work of the London Resilience Partnership. Local Resilience Forums were introduced in 2004 in the Civil Contingencies Act to provide the means for those involved in emergency preparedness to collaborate at a local level.

The LRF ensures London's preparedness in the event of emergencies and coordinates the activities of a wide range of organisations to achieve this. It also provides a link between emergency preparedness and resilience at the local and national levels.

The London Resilience Partnership comprises more than 200 organisations. These include local authorities, emergency services (police/fire/ambulance/coastguard), health organisations, utility companies, transport providers, and representatives of the business, faith, and voluntary sectors.

As well as the LRF, a Borough Resilience Forum (BRF) is maintained in each London Local Authority area. The Borough Resilience Forums enable cooperation and information sharing between resilience partners to support emergency preparedness at the Borough level.

The LRF and BRFs maintain a range of emergency response capabilities that will be supported by this Data Sharing Agreement (DSA), such as those set out in the London Humanitarian Assistance Framework, and Borough-level arrangements to provide humanitarian assistance to people affected by an emergency. These arrangements would be coordinated by a Humanitarian Assistance Steering Group (HASG) established for the emergency which would agree information sharing requirements between HASG members as required to support the humanitarian response.

This DSA documents how the parties to this agreement will share personal data about people affected by an emergency with organisations that have a responsibility to undertake safeguarding actions and/or offer or provide support services to those people, such as humanitarian assistance. Examples of actions and support services for which information may be shared include:

- warning and informing the public
- evacuation
- provision of rest centres, survivor reception centres, family and friends reception centres
- immediate medical treatment, health and social care
- longer-term health care (mental, physical and public health) and social care
- assistance with temporary accommodation
- financial and practical support
- bereavement support
- Casualty Bureau Receives information relating to persons who are believed to have been involved in an emergency

Data sharing is necessary for criminal and civil investigation purposes to:

- reduce immediate or short-term risk of continuation of the incident or a similar incident, where the incident is impacted by criminal activity.
- reduce potential fraud such as fraudulently seeking humanitarian or financial support.
- identify and interview victims and witnesses.

Outside of the immediate incident response, the sharing of information may be required to:

- support humanitarian assistance for a long period of time following an emergency. For example, long-term health care, support to people during inquests, memorials, and anniversaries.
- prepare for a potential emergency by identifying individuals likely to need support during an incident.
- reduce likelihood of fraud, or future incidents impacted by criminal activity.

The sharing of information may also be required if an emergency is likely to occur (i.e. prior to an emergency). For example to identify and provide support to vulnerable persons who may be affected by a forecast flooding emergency and require additional support services.

There are practices in place between some organisations to share or maintain joint lists of vulnerable persons regularly for emergency preparedness activity, i.e. rather than only gathering this information at the time of an emergency. Such information is also shared between some organisations to inform priority services for vulnerable customers, for example those offered by utility companies. These practices are related to sharing information about people affected by an emergency, however, they are not covered by this Data Sharing Agreement.

The categories of people affected by an emergency, or data subjects, include injured survivors, non-injured survivors, witnesses, bereaved family and friends, and emergency responders (see section 3.3. for full list).

Data to be shared may include personal information (e.g. name and contact details), how the person is thought to have been affected (i.e. their data subject category e.g. injured survivor), and special category data (e.g. known vulnerability or medical need).

Data would be shared between two or more organisations with a responsibility to offer or provide support services to the data subject.

The organisations party to this Agreement are listed in Appendix A, and the agreement is to be signed by all relevant parties, including local partners, voluntary sector, and any specialist organisations.

By signing this Agreement, the named agencies agree to accept the conditions set out in this document, according to their statutory and professional responsibilities, and agree to adhere to the procedures described.

This Agreement has been developed to:

- Define the specific purposes for which the signatory agencies have agreed to share information.
- Outline the Personal, Special Category and Criminal Data to be shared.
- Set out the lawful basis conditions under UK General Data Protection Regulations (GDPR) and Data Protection Act 2018 through which the information is shared, including reference to the Human Rights Act 1998 and the Common Law Duty of Confidentiality.
- Stipulate the roles and procedures that will support the processing/sharing of information between agencies.
- Describe how the rights of the data subject(s) will be protected as stipulated under the data protection legislation.
- Describe the security procedures necessary to ensure that compliance with responsibilities under data protection legislation and agency-specific security requirements.
- Describe how this arrangement will be monitored and reviewed.
- To illustrate the flow of information from referral through processing and outcome.

Parties to this agreement cannot amend or add appendices unless agreed as part of a formal review. It is expected that each party will have procedures, processes and policies sitting underneath this agreement, for their respective organisations. These will, for example, describe the specific processes for secure transfer of data.

1.1 Ownership of this agreement

This agreement was drafted by a working group of representatives of the police services, London Fire Brigade, health sector, London local authorities and London Resilience Group. These professionals were specialists in resilience, safeguarding, social work, police procedures, information governance and law. The local authority representatives worked under the banner of the Information Governance for London Group (IGfL), to draft one agreement that would work for all Local Authorities, CCGs and police BCUs across London. The aim is to reduce the number of versions of sharing agreements that historically differed between boroughs, partly to reduce the burden on pan-London organisations that must have agreements with multiple boroughs.

IGfL, a group of information and security professionals at London local authorities, assisted with coordination of this agreement, but the responsibilities within it, and compliance with data protection legislation, remain with the listed data controllers.

1.2 Responsibilities of parties involved

The parties are registered Data Controllers under the Data Protection Act 2018 and as such are recognised within this agreement as Data Controllers in their own right. Signatories are identified as those who have signed this agreement on the Information Sharing Gateway or through local sign-up processes. A list of expected types of signatories is at Appendix A.

All parties confirm that they comply with data protection legislation by:

- having a lawful basis for processing and sharing personal data.
- ensuring data quality.
- storing and sharing information securely, with access management controls.
- having policies and procedures for compliance with data protection legislation including for managing data subject rights & complaints, identifying and managing data breaches/incidents and retention & disposal.
- ensuring that mandatory training is undertaken regularly by their employees to ensure they are clear and up to date on their responsibilities. Every individual must uphold the principles of this agreement and overarching confidentiality, and seek advice from the relevant Data Protection Officer when necessary.
- undertaking appropriate data protection due diligence checks with any contractors/data processors they employ, and ensuring that a written agreement is in place with each data processor, and that all data processors will be bound by this agreement.
- having written processes for the processing of data to ensure employees use and share personal data in line with data protection law, the data protection principles, and this agreement.

Organisations and their staff must consult the organisation's Data Protection Officer/Information Governance Manager and/or Caldicott Guardian if they are unsure at any point in the processing and sharing of personal data.

1.3 Confidentiality and vetting

Each Partner must ensure that there are appropriate written contracts or agreements with employees, agency staff, volunteers etc. These must include requirements to ensure compliance with policies which include confidentiality.

Each Partner must ensure that suitable vetting has taken place. This may be through standard employee checks (BPSS or equivalent), DBS, Security Vetting or Counter Terrorist Check [CTC].

1.4 Assessment and review

A review of this information sharing agreement will take place after six months and yearly thereafter, unless otherwise agreed by the organisations' Data Protection Officers. The aim of the review will be to ensure the purposes are still relevant, the scope has not changed, the benefits to the data subjects and organisations are being realised, and the procedures followed for information security are effective. The agreement will therefore also be reviewed if relevant learning is identified by the London Resilience Partnership from the debrief of a Major Incident or Emergency affecting London.

Changes in legislation and developments in the areas of public sector data sharing will be considered as and when they arise, as will any changes to the signatory parties. Specifically, any revision of 'HM Government 2021 Data Sharing in Emergency Preparedness, Response and Recovery. Non-statutory guidance on the sharing of Personal and Special Category Data during all phases of an emergency will be considered.

The working group who drafted this agreement strongly recommend that a working group approach is used for any reviews, as this was a successful way to achieve pan-London and cross-specialism consensus to a single data sharing agreement.

The review working group will be facilitated by London Resilience Group. All organisations party to the agreement will be invited to participate (either directly or represented on a sector basis as per the London Resilience Forum structure). Any other relevant organisations will also be invited e.g. those involved in making use of the Agreement in response to an emergency which has prompted the need for the Agreement to be reviewed.

1.5 Termination of agreement

In the event of termination of this agreement each party may continue to hold information originating from other parties for which they are the Data Controller.

2. Purpose and Benefits

Sharing information between partner organisations in an emergency is vital to the provision of coordinated and seamless humanitarian assistance services to support people affected. People affected can include survivors, family/friends of those missing, killed or survivors, witnesses and the affected communities. Sharing can help to meet the requirements of statutory legislation, government guidance, London Resilience Partnership Frameworks such as the Humanitarian Assistance Framework, and local organisational arrangements.

These services include activities aimed at addressing the needs of people affected by emergencies in terms of the provision of psychological and social aftercare and support in the short, medium and long term.

The types of emergencies which may require these services include (but are not limited to):

- accidents and system failures (e.g. utilities or transport failures)
- human and animal diseases (e.g. flu pandemic)
- societal risks (e.g. public disorder)
- natural hazards (e.g. flooding)
- hostile state activity (e.g. cyber-attacks)
- threats (e.g. terrorist attacks)

A full list of risks of emergencies is provided in the London Risk Register.

This Data Sharing Agreement (DSA) sets out the overarching information principles between those listed in Appendix A, in sharing data in the event of an emergency or major incident. This DSA aims to:

- Assist in the provision of appropriate and timely assistance to people affected in the short, medium and longer term
- Ensure a seamless approach to the provision of assistance between partner organisations and avoid duplication
- Collate information to enable the identification and prioritisation of those in need of assistance
- Assist in decision making and prioritising resources to assist those most in need

This DSA supports a range of London Resilience Partnership frameworks, protocols and capabilities, for example those set out in the Humanitarian Assistance Framework, Recovery Coordination Protocol and Identification of the Vulnerable Guidance. It also supports associated plans which exist beneath these at the Borough/local and organisational level.

Decisions must be made quickly in emergency situations, but this does not mean we can ignore our responsibilities for protecting and sharing personal data. Each protection/sharing decision is unique, but the process by which those decisions are made should be established in advance.

Plans can be made for how to protect and share data in likely scenarios, which will support staff on the ground and in command, to make effective, timely and appropriate decisions. For example:

- Evacuations
- Survivor reception centres and rest centres
- On location support
- Identifying actual or potential victims
- Immediate and follow up welfare support or treatment
- Family support or bereavement locations

Outside of the immediate incident response, the sharing of information may be required to:

- support humanitarian assistance for a long period of time following an emergency. For example, long-term health care, support to people during inquests, memorials, and anniversaries.
- prepare for a potential emergency by identifying individuals likely to need support during an incident.
- help organisations identify individuals that may require wider future support e.g. ongoing social care and utility priority service registers.
- reduce the likelihood of a repeat or similar incident.
- plan for effective data sharing for future incidents e.g. agree definitions of vulnerability across organisations, or establish routes for data matching and ensuring suitable data quality.

Parties to this agreement have requirements under the Civil Contingencies Act 2004 to prepare for emergencies, which includes preparing to easily and quickly identify those individuals in need of support. This can be a 'List of Lists', which is non-personal data that details where information on vulnerable individuals can be found, or it can be personal data. If personal data, this may be drawn from within local authority safeguarding case files, or utility company Priority Service Registers for example. There are practices in place between some organisations to share or maintain lists of vulnerable persons regularly for emergency preparedness activity. The parties to this agreement recognise that this is encouraged by the Ofgem and Ofwat regulators.

Data collected during an emergency response may allow organisations to identify or update their records of individuals needing support outside an emergency incident, whether utility company Priority Service Registers or local authority child and adult safeguarding casework. The parties recognise that this could be justified as part of the parties' public tasks, and substantially in the public interest (where using special category data). The necessity and benefits for sharing this data will change between types and severity of incident, and data sharing channels may be developed under this DSA to support this work.

As part of work to reduce the likelihood of future incidents, the parties can consider sharing data to change processes or locations. Often non-personal or pseudonymised data could be used, and examples include use of footage and witness statements to change buildings and locations for better emergency evacuation, or install environmental remediations such as flood barriers.

2.1 Benefits

The overall benefit of this DSA is to improve the outcomes for those people affected by an emergency. It will do this by:

- Enabling the sharing of information for the purpose of identifying people affected by an emergency and offering and providing appropriate services to them.
- Setting parameters for sharing personal data and clearly identify the responsibilities of organisations.
- Identifying the correct lawful basis to share personal information.
- Ensuring information is shared whenever there is a requirement to do so.
- Removing barriers to effective information sharing.
- Avoiding duplication of effort.

- Raising awareness amongst all partner organisations of the key issues relating to information sharing and give confidence in the process of sharing information with others.

Benefits of the data sharing itself include:

Individuals

- Warning and informing of potential or actual emergency incidents
- Help to evacuate
- Support during an incident for example, humanitarian support such as rest centres/accommodation, immediate and longer-term health care and social care, access to information, bereavement support, financial and practical support

Organisations

- More effective use of resources
- Ability to better plan for incidents
- Clarity on responsibilities to avoid duplication or gaps
- Reduction in likelihood of future incidents
- Safeguard staff and volunteers engaging with persons affected by incidents

Society

- Effective and timely management of emergency incidents and ongoing issues
- Effective use of resource, people and financial, to manage incidents and support individuals
- Reducing duplication of effort or gaps in service provision
- prepare for a potential emergency by identifying individuals likely to need support during an incident.
- Reduce likelihood of fraud, or future incidents impacted by criminal activity

2.2 Principles of information sharing

Effective information sharing is a vital element of the provision of appropriate services to people affected by an emergency.

To share information, a lawful basis for doing so must be identified. This may come from legislation or from statutory guidance such as the national guidance Data Sharing in Emergency Preparedness, Response and Recovery.[1]

The sharing of personal data must comply with both the GDPR Principles and the Caldicott Principles (where applicable), listed at Appendix B. Together, those principles lead to a series of questions and considerations to be answered before sharing takes place. These are listed in Appendix D: Information Sharing Checklist.

2.3 Who can share personal data?

Data protection legislation does not prevent any organisations sharing information in an emergency. Public bodies, voluntary organisations, private organisations, and any other bodies who may be called upon in emergencies all have the ability to share personal data provided that they have a lawful basis to do so, and sharing is in accordance with data protection legislation, including the data protection principles.

[1] Non-statutory guidance on the sharing of Personal and Special Category Data during all phases of an emergency.

2.4 Legal powers to share personal data

The first data protection principle requires data to be shared lawfully. For public sector bodies this means they also need a power to share data.

The Civil Contingencies Act 2004 requires Category 1 and 2 responders to prepare for emergency incidents. For these responders, the Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005 provide a legal power to share personal data. Regulation 44A allows responders to share information with one another in connection with the performance of their functions under the Act.

Regulation 47 gives responders the right to request information from other responders in relation to their duties under section 2(1)(a)-(d) (duty to assess, plan and advise on emergencies) and section 4 (duty to provide advice and assistance to the public) of CCA 2004, or in connection with the performance of other functions that relate to an emergency, where they don't have the information themselves and it is not reasonable to obtain it by other means. If the conditions in regulation 47 are met and the request is made in accordance with the procedure in regulation 48 the starting point is that the responder who receives the request must share it. An exception applies in relation to "sensitive information" as defined in regulation 45. This includes information that would prejudge national security, public safety, commercial interests and information which, if shared, would contravene data protection legislation as applied by regulation 45 1A – 1E.

However, using the sharing powers within the CCA Regulations are not considered the first line of approach. There are multiple pieces of legislation that provide a lawful basis for emergency responders to share data.

Public bodies like local authorities, police forces, utility companies, transport providers and NHS Trusts have statutory expressed or implied powers to share personal data as part of their duties. A government department acting under the authority of a Minister may be able to share data using common law powers.

For voluntary organisations and private organisations, a legal power to share personal data simply means it must not be prohibited by law. There are lawful bases that will apply, likely with a public interest test required. Proportionality and necessity tests provide support for whether sharing the data is 'fair'.

2.5 Lawful Basis

In addition to identifying relevant legal powers, data sharing must comply with the data protection legislation, including the data protection principles.

The first principle requires data to be shared fairly and lawfully. This means not breaching any other laws (for example the common law of confidentiality or the Human Rights Act 1998 (in particular the right to a private life under Article 8 of the European Convention on Human Rights).

It also means that organisations must identify valid grounds to share personal data (known as a 'lawful basis') and additional grounds to share special category data (known as 'conditions'). A large majority of the instances when organisations involved in preparing for, responding to, and recovering from emergencies will seek to share personal data, will be measures to protect individuals from harm. This is likely to particularly focus on individuals at increased risk of harm, due to either pre-emergency, identified vulnerabilities, or due to the impact on them of an emergency in which they are involved.

The sharing of information must comply with the laws relating to confidentiality, data protection and human rights. Having a legitimate purpose for sharing information is an important part of meeting those legal requirements. This is a complex area, and each partner organisation must take their own decisions and seek advice from their organisation's Data Protection Officer/Information Governance Manager and/or Caldicott Guardian (where relevant).

2.5.1 Processing personal data for law enforcement purposes

Part 3 of the DPA 2018 relates to the processing of personal data by a competent authority (as defined in Section 30(1) and Schedule 7 of the DPA 2018) for law enforcement purposes. "Law enforcement purposes" are defined in Section 31 of the DPA 2018 to mean "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

The powers to share such information are set out in Section 2.4 above.

This regime will be applicable to processing undertaken by competent authorities (e.g. the police) that are processing data for law enforcement purposes. This will apply where, for example, the police wish to contact a partner body to establish the location of a specific individual who is (or may be) a victim, witness or suspect connected to a criminal act.

It is possible that the police may not have a name for the person or people that they are seeking, but are only able only able to identify an individual using a description of his/her physical appearance. In such cases the police may provide details of the individual which would amount to sensitive processing within the definition of Section 35(3) of the DPA 2018.

In order for competent authorities to carry out and share sensitive personal data with partners:

- that processing must be strictly necessary; and
- at least one condition specific in Schedule 8 of the DPA be satisfied. An analysis of three relevant conditions is set out below:

Strict necessity

Although it is difficult to anticipate all the circumstances in which sharing under this agreement may be necessary, in general competent authorities do not consider that there are any other less intrusive means of obtaining personal data held by partners.

The reasons for the necessity of sharing personal data is set out in Sections 2 and 2.1 (above) and 2.6 (below).

Schedule 8 conditions

The following conditions set out in Schedule 8 of the DPA 2018 are likely to be satisfied, depending on the precise context of the data processing:

Paragraph 1: Statutory etc purposes

This condition is met if the processing—

(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and

(b) is necessary for reasons of substantial public interest.

The processing of the data is carried out in the exercise of the legal powers and duties of the MPS. It is plainly in the substantial public interest that for example witness, victims and potential suspects are located as soon as reasonably practicable by the police.

Paragraph 3: Protecting individual's vital interests

This condition is met if the processing is necessary to protect the vital interests of the data subject or of another individual.

This condition is met in cases where there is a risk to the life of the of the data subject or where the data subject poses a threat to the life of either his or herself or the life of others. This may be the case where the police consider that a victim faces an ongoing risk of harm.

Paragraph 4: Safeguarding of children and of individuals at risk

(1) This condition is met if—

(a) the processing is necessary for the purposes of—

(i) protecting an individual from neglect or physical, mental or emotional harm, or

(ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is—

(i) aged under 18, or

(ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual—

(a) has needs for care and support

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

This condition is met where the child or vulnerable adult is at risk of harm (whether physical or mental), and the police are unable to obtain consent for any of the reasons listed in para 4(2). This condition will be met in most cases given the serious risk of harm posed to missing children or vulnerable adults in the aftermath of a major incident.

The terms of this agreement address the requirements for data sharing pursuant to Part 3 of the DPA 2018.

To note that there is a separate regime for intelligence service processing, which falls outside the remit of this DSA.

2.5.2 For purposes other than law enforcement by competent authorities

Articles 6, 9 and 10 of the UK GDPR, and section 8 of the DPA 2018 set out the acceptable conditions for the processing and sharing of personal, special category, and criminal data. The conditions relevant in the UK GDPR to data processed under this agreement are below.

A Note on Consent

The parties will often work collaboratively with data subjects and aim for agreement with them on the actions to be taken. However, it is recognised that this is different to using consent (Article 6 (a)) or explicit consent (Article 9 (a)) as the lawful basis conditions used for processing under this agreement.

Consent is not generally the lawful basis the public sector organisations use for processing information shared under this agreement. It is possible that the other parties, such as voluntary groups, may use consent as lawful basis for some personal data processing. Each party is responsible for managing consent where they use consent as the lawful basis condition.

Lawful Basis for processing Personal Data. The lawful bases for sharing Personal Data that are likely to be most relevant to organisations involved in resilience will be:

Public Authorities

- **Article 6(1)(c) – legal obligation***:* processing is necessary for compliance with a **legal obligation** to which the controller is subject. Organisations may have a legal obligation to share data, especially in relation to children and safeguarding.

- **Article 6(1)(e) – public task:** (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. (Use of this article requires that the Data Protection Act section 8 be satisfied, the underlying task, function or power must have a clear basis in law, though that need not be statutory, it could be based on common law or part of a contractual obligation. The laws given in this DSA Appendix B – Applicable legislation provide for each party a legal basis under section 8 – the specifics are noted in the appendix). This is likely to be the most relevant lawful basis for sharing.
- It is highly likely that most data sharing under this DSA will fall within Article 6(1)(c) or (e)
- **Article 6(1)(d) – vital interests:** where processing is necessary to protect the data subject's life or the life of another person. This is unlikely to be a common basis. For more detail see the ICO's guidance on vital interest.
- **Outsourced or contracted services**. Where there is sharing by a contracted organisation, whether a company, public sector body, or voluntary organisation, where there is a formal relationship regulating the parties' relations and the contracted party is Data Processor of the public authority, the sharing by the Data Processor will be under the lawful basis of the Data Controller.

Private or Voluntary Organisations

- See note above about the position regarding private and voluntary sector organisations which are Data Processors of the Data Controller
- Where the private or voluntary sector organisation are acting as a Data Controller their legal basis is likely to be:
- **Article 6(1)(f) - legitimate interest.** In order to meet the legitimate interest basis, private and voluntary organisations need to: identify a legitimate interest; demonstrate that the sharing of data is necessary to achieve that interest; and then balance that interest against the individual's interests, rights and freedoms. These interests can include broader societal benefits such as protecting individuals from harm. Relevant will be the reasonable expectations of the individual, taking into account their relationship with the organisation processing their data. Where an organisation, such as a public authority, requests data sharing from another body, to allow the requester to deliver its duties, it can be considered in the legitimate interest of the other body to share the data.
- **Article 6(1)(e) – public task:** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This can apply if an organisation is either: 'Carrying out a specific task in the public interest which is laid down by law; or exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law'. For example a private water company fulfilling its public duties, or a voluntary organisation fulfilling a duty for a public body where that voluntary organisation is a Data Controller.

  To rely on 6(1)(e) - public task the underlying task, function or power must have a clear basis in law, though that need not be statutory, it could be based on common law or part of a contractual obligation. This is explained in detail in the ICO guidance.
- **Article 6(1)(c) – legal obligation**: processing is necessary for compliance with a legal obligation to which the controller is subject. Organisations may have a legal obligation to share data, especially in relation to children and safeguarding or may be fulfilling statutory responsibilities eg a utility company.
- **Article 6(1)(d) – vital interests**: where processing is necessary to protect the data subject's life or the life of another person. This is unlikely to be a common basis. For more detail see the ICO's guidance on vital interest.

When organisations share personal data they must do so in a "transparent manner" in accordance with the data protection principle in Article 5(1)(a).

Lawful Basis for Processing Special Category Personal Data

In order to lawfully share special category personal data, both an Article 6 lawful basis as set out above, and one additional condition for processing data from Article 9(2) GDPR must be met. As with Article 6, only a single condition for sharing special category personal data must be met – having more than one applicable condition does not make the sharing of data any more legitimate. More information and advice on sharing special category data can be found on the ICO website.[2]

The following conditions are considered to be most relevant to this DSA. **Article 9 (2) – Special Category Personal Data Processing**

- **Article 9(2)(c) processing is necessary to protect the vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent. This will only be a relevant condition for sharing in life-or-death scenarios. There is also a higher bar to meet here than in the Article 6 lawful basis, in that persons in question must also be physically or legally incapable of giving their consent to their special category personal data being shared. If there is another lawful basis that applies, which is likely given the duties and powers of parties to this agreement from their specific legislation, then this should be used rather than vital interests.
- **Article 9(2)(g) substantial public interest** - processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. This is likely to be the most relevant condition.
  One of the conditions in Part 2 of Schedule 1, Data Protection Act 2018 needs to be met. Likely conditions under Part 2, Schedule 1 are:
  - para 6 Statutory etc and government purposes,
  - para 10 Preventing or detecting unlawful acts, or
  - para 18 Safeguarding of children and of individuals at risk.

The organisation must have an 'appropriate policy document' in place that explains the controller's procedures for securing compliance with the principles in Article 5 GDPR.

For some of the conditions in Schedule 1, there is a need to justify why obtaining explicit consent is not possible. Data subjects having their data processed for emergency resilience purposes are vulnerable and there is an imbalance of power between data subjects and data controllers. It is not considered that truly informed and freely given consent can be achieved, especially as consent could not be withdrawn for the processing undertaken under this DSA. It is also not considered practical to expect data controllers to seek consent for data processing during fast-moving emergency incidents.

- **Article 9(2)(h) provision of health or social care** - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- **Article 9(2)(i) public health -** processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

  This is likely to be a suitable lawful basis for incidents involving disease spread such as influenza or Legionnaires'; for the spread and impact of radiation poisoning; or danger to health from sewage infiltrating water supplies.

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Lawful Basis for Sharing Criminal Offence Data

Art. 10 GDPR: Processing of personal data relating to criminal convictions and offences states that processing of personal data relating to criminal convictions and offences or 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.

Article 10 requires that an article 6 condition is met- this is likely to be the same as the article 6 basis for processing personal data. It also requires that a condition in Part 1 or 2 of Schedule 1 Data Protection Act 2018 is met. The most relevant conditions will be:

- Part 1 para 2 Health or social care purposes,
- Part 2 para 6 Statutory etc and government purposes
- Part 2 para 10 Preventing or detecting unlawful acts
- Part 2 para 18 Safeguarding of children and of individuals at risk.

2.6 Proportionality and necessity

Proportionality and necessity are factors to be taken into consideration when deciding whether to share personal information. In making the decision, employees must weigh up what might happen as a result of the information being shared against what might happen if it is not, and apply their professional judgement.

Organisations party to this Agreement are expected to justify that they believed sharing was necessary for one of the following criteria:

- necessary for the purposes of preventing or detecting crime
- required or authorised by an enactment, by a rule of law or by the order of a court or tribunal
- in the particular circumstances, was justified as being in the public interest.

Or that the organisation acted in the reasonable belief that:

- the person had a legal right to do the obtaining, disclosing, procuring or retaining
- the person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it

What is considered ‘reasonable’ will change depending on the circumstances. For a rapid response to emergencies, or getting immediate physical, mental and emotional support to those affected, organisations will have to make quick judgements. It is recommended that all parties consider likely sharing needs and establish protocols as part of their emergency preparedness, so that employees and practitioners are confident in making lawful decisions quickly.

2.7 Other relevant legislation

The actual disclosure of any personal data to achieve these objectives must also be conducted within the framework of the Human Rights Act 1998 (HRA) and the Common Law Duty of Confidence. Caldicott Principles also apply to all information sharing and they are listed in Appendix B: Data Protection & Caldicott Principles.

- Human Rights Act 1998 (HRA)
- Common law duty of confidentiality
- Confidentiality and Sharing for Direct Care

2.8 Common Law Duty of Confidence

Information may have been gathered where a duty of confidence is owed. Duty of confidence is not an absolute bar to disclosure as information can be shared where consent has been provided or without consent where there is a strong enough public interest to do so. Whilst applying proportionality and necessity to the decision, the protection of vulnerable persons fulfils a public interest test when passing the information to a partner agency whose work would facilitate this aim.

When overriding the duty of confidentiality, the parties may seek the views of the organisation who hold the duty of confidentiality and consider their views in relation to breaching confidentiality. The organisation may wish to seek legal advice if time permits. While desirable, depending on the circumstances and urgency it may not be proportionate to seek the agreement of the organisation who hold the duty of confidentiality or legal advice.

2.9 Freedom of Information (FOI)

The Freedom of Information Act 2000 gives all individuals the right to access official information held by a public authority (the Environmental Information Regulations 2004 also allow access to data. For ease of drafting, FOI is used to cover both legislation). Limited exemptions may apply, and all public authorities must ensure they have recognised procedures in place for administering requests of this nature.

All requests for FOI will be directed through the relevant organisations' FOI processes. Each party will seek advice/opinion from the other parties where there is concern about that information being released and any impact it is likely to have. The final decision to disclose or not will lie with the party who has the legal duty to respond to the request.

It is encouraged that all parties proactively publish this document. It may also be disclosed to the public under FOI.

3. Individuals

Organisations processing personal data are required to begin with the ethos of Data Protection by Design and Default (also known as Privacy by Design (PbD)). This means that we must consider and uphold the privacy of an individual's data before we begin and throughout the processing taking place.

Each party agrees that they have undertaken a DPIA (Data Protection Impact Assessment), where they feel the processing meets the legislative criteria for a DPIA.

3.1 Right to be informed – Privacy Notices

Where personal data is created or received by one of the parties, they are responsible, as required by law, for making the data subject(s) aware within a reasonable time frame that the organisation holds the data, what they will do with it, how long they will keep it, and who they will share it with (such as under this DSA). This is normally done through a privacy notice, whether written or verbal. Organisations agree that they will adhere to the transparency requirements of the UK GDPR and will issue appropriate notices which inform the data subject that the information will be shared with the parties under this agreement.

In some cases, it may not be appropriate to let a person know that information about them is being processed and shared. Consideration should be given to whether notifying the individual may place someone at risk or prejudice a police or safeguarding investigation. In these circumstances, the parties need not inform individuals that the information is being processed/shared; but should record their reasons for sharing information without making the individual aware.

We must be practical and recognise that whilst privacy information is required, it should be suited to the circumstances. It is unlikely to be useful to hand out full privacy notices during an incident, but there are options available.

Privacy information can be provided on websites and within emergency preparedness plans, so the public are aware overall of the types of data shared during emergency incidents. Parties to this agreement must ensure they create suitable privacy information as part of their emergency preparedness, that can be employed

during an incident. For example, a short, clear explanation for display in rest centres, and privacy information given at the same time as follow up support. Where deemed appropriate, template privacy notices will be developed to provide a standardised approach across London. The London Humanitarian Assistance Framework includes guidance and templates.

3.2 Data subject rights requests and complaints

Each organisation must have in place appropriate policies and processes to handle data subject requests made in line with data protection law, to ensure they are responded to within deadline and in an appropriate manner. Requests include; right of access, right to rectification, right to erasure, right to restrict processing, right to data portability, right to object and rights related to automated decision making including profiling.

If an individual successfully requests the erasure or limitation of use of their data (right to erasure, right to rectification, right to restrict processing, right to object), the party that has been informed by the data subject will communicate this to the other parties where relevant and appropriate. In each case each party is responsible for securely disposing of such information or limiting its processing.

Each party must have clear, fair, and objective complaint procedures. Any complaints from individuals how their data is being processed or shared will be handled under the policy and processes of organisation concerned.

3.3 Data subject categories

The data subjects whose data is shared under this agreement include the following:

- Children
- Adults
- Injured survivors
- Non-injured survivors
- Witnesses
- Bereaved family and friends
- Concerned family and friends of people directly impacted by the incident
- Displaced people
- Responders (employed and community)
- People in the community / local area directly and not directly affected by the incident
- Actual or suspected perpetrators

Data is shared on employees of relevant organisations such as local authorities, emergency responders and utility companies, where this is necessary to coordinate and deliver support to those in need.

Many of the data subjects may be vulnerable. Parties to this agreement are in positions of power over data subjects and data subjects have little or no control over why and how their data is processed.

4. Data

The personal data and its processing involved in supporting people affected by an emergency is sensitive and of vulnerable individuals.

There may be a high volume of data and data subjects.

Anonymisation or pseudonymisation will rarely be possible because of the way the work focusses on individuals, although any statutory returns, workforce planning and management reports should be anonymised if possible.

4.1 The data to be shared

Due to the complexity of the work involved in the subject of this DSA, providing a prescriptive list of data fields to be shared is difficult. Not all the information will be shared in every case.

Examples of personal and special category information that may be shared is listed below but this is not an exhaustive list.

- Name
- Address and postcode
- Telephone number (landline / mobile)
- Date of birth
- Age
- Gender
- Data subject category (e.g. injured survivor)
- Nature of support required
- National Insurance number
- NHS number
- Nationality, ethnicity and languages spoken
- Equalities information, for example where religious beliefs affect how support can be provided to an individual
- Medical information including support required and vulnerabilities
- GP name and practice contact details
- Social care information
- Care/service providers
- Housing information
- Family/relationship information including support network and contact details of family members or significant others
- Property information
- Financial information
- Criminal allegation and prosecuting information
- Employment information
- Images and footage including CCTV, dashcam and body worn footage (noting there is also a specific CCTV DSA)
- Information held in agencies caution registers or similar which are a database of information about properties or individuals where a risk is posed to visitors due to the inhabitants or conditions in the property

4.2 Deceased persons

It is noted that the sharing may involve data of deceased persons. This data will not be covered by data protection legislation but will still require due regard to the common law duty of confidentiality and the Human Rights Act.

4.3 Confidential information

In this agreement, we refer to personal data, as defined by data protection legislation. However, the word 'confidential' may be used by individuals and practitioners to describe information and can mean different things to different people.

Confidential can mean:

- Personal and special category data as defined by data protection legislation
- Patient Identifiable Information (PII) or 'personal confidential information'; both terms most commonly used in health settings
- Information which is not already lawfully in the public domain or readily available from another public source
- Information that has been provided in circumstances where the person giving the information could reasonably expect that it would not be shared with others.

4.4 Storing and handling information securely

Information must be stored and shared lawfully and securely. Special category data may need a higher level of security. The employee/organisation sharing the information must choose the most appropriate secure method of transfer and be responsible for its safe delivery. Parties must make sure the chosen method is suitably secure and that access is only provided to those who need it, and only to the data needed.

Parties must plan for likely scenarios and establish the most secure way to keep and share personal data during incidents. This might mean:

- including rugged tablets for frontline roles or rest centres to avoid needing to use paper forms
- lockable cases for transfer of paper
- secure sharing routes and email accounts prepared for use in an emergency with details in preparedness plans

Electronic records:

Organisations may have different electronic methods for storing and sharing information securely. Some have local restrictions which block access to information shared using specific tools. There must be protocols and staff training to ensure that these records are kept safe, and confidential. Many of the parties to this agreement will have PSN (Public Services Network) or DSPT (Data Security & Protection Toolkit – NHS) accreditation, which means they have proven suitable approaches to data protection and security. Parties must consider these standards

Unencrypted email (i.e. sent in plain text over the public internet) must not be used to share information under this DSA.

Sharing methods that may be appropriate include:

- **Email encryption tools** where the email and attachments are encrypted from named sender to named recipient (e.g. Microsoft 365 Message Encryption; Egress Protect)
- **Encryption via Transport Layer Security** (TLS) where the email and attachments are encrypted in transit over the internet. Both the sender and recipient email domains must have TLS enabled. This can be checked using https://www.checktls.com/
- **Secure corporately managed data repository and sharing platforms** (e.g. MS Teams; Google Docs)
- **Secure group email services** (e.g. CJSM: https://cjsm.justice.gov.uk/index.html)
- **Secure File Transfer Protocols**
- **Virtual Private Networks**

The above are examples. Parties to this Agreement should get advice from their organisation's information security or IT teams on secure methods of sharing available at your organisation and document these in the organisation's process documents.

For police information about people affected by an emergency, the Major Incident Public Portal (MIPP) may be used. MIPP, found at mipp.police.uk can be used by anyone to submit information on any device. Utilising this system allows anyone to report people missing as a result of mass casualty incidents. They can also cancel missing person reports or provide information directly to the incident room. MIPP will also be used by documentation teams to provide information about those involved in the incident to the Casualty Bureau. The system is a secure, encrypted portal – with the data stored within only accessible through, specifically trained managers within the Casualty Bureau. Prior to the launch of MIPP or Casualty Bureau for an incident, the default for sharing of information with Police will be via "business as usual" routes with Met CC. Should MIPP or Casualty Bureau be opened, or another information sharing process be established by MetCC (e.g.: the tri-service call between emergency service control rooms) for an incident then MetCC will communicate this to relevant partners.

Phone/virtual meetings/face-to-face meetings:

Information may be shared over the phone, in a virtual meeting, or at face to face meetings. Meeting attendance and distribution of content, e.g. meeting minutes or recordings, must be limited to those with a need to know.

Sharing by telephone should be avoided unless the requirement is urgent and email is not practicable.

Individuals should be aware of their surroundings and the presence of other individuals or voice recognition or 'Internet of Things' devices (e.g. virtual assistant apps like Alexa, Cortana, SIRI) to ensure they aren't overheard by those that should not have access to the information discussed.

Paper records:

Printed paper records must always be kept to a minimum and kept secure whether in the office, home or during transit. Organisations must adopt an appropriate policy surrounding the use and transfer of paper records. Appropriate security methods must be applied when storing or disposing of paper records.

4.5 Access controls and security

All parties will ensure that they have appropriate technical and organisational security measures in place to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

All personal data held by partner organisations electronically will be stored in a secure network area with password protected entry and appropriate back-up functionality. The systems will be auditable so that it is possible for any auditor to establish who has accessed the system. All laptops, computers, and any other portable devices will be encrypted.

Any individual no longer required to have access will promptly have such access revoked by the line manager and Human Resources related to the relevant employer.

There is an expectation that partner organisations will either be working toward ISO 27001, the International Standard for Information Security Management, or a similar standard of security.

4.6 Outside UK processing

Parties are responsible for ensuring that if information is processed or shared outside the UK, that suitable written agreements are in place, and that appropriate due diligence has been completed for the transfer of data.

4.7 Data quality

Each partner is responsible for ensuring the accuracy and relevance of the personal data that it processes and shares and must have clear processes in place for managing data quality. This is especially important in emergency incidents where those at risk and their families are vulnerable and in need of immediate, appropriate assistance.

Any party learning of the inaccuracy of personal data is responsible for informing the parties with whom that data has been shared.

The Cabinet Office guidance 'Identifying People Who are Vulnerable in a Crisis'[3], defines a vulnerable person as 'a person less able to help themselves in the circumstances of an emergency.' It is however important to note that 'while all people caught up in an emergency could be (and in some circumstances will be) defined as vulnerable due to their proximity to the event, planning and response arrangements should focus on those who are assessed as not being self-reliant and may need external assistance to become safe.' (Cabinet Office, 2008).

Each organisation will identify and describe 'vulnerability' differently. For example, utility companies and local authorities will have different vulnerability categories. It is recommended that preparedness work considers this so that exchange of usable data can be as smooth as possible during an incident. Each organisation must consider the best way to match personal data from multiple sources, and how to improve data quality.

Another area of concern for data quality is that organisations use different addressing data systems, or none in some cases. Parties are recommended to consider the use of addressing in their systems and information to establish consistency, with use of UPRNs (Unique Property Reference Numbers).

4.8 Data breaches/incidents

All parties must have a clear policy and procedure regarding the reporting and handling of data protection breaches or data loss incidents. It is recommended that parties consider where normal processes may need to adapt for data protection incidents that occur during emergency incidents. Priority must be given to safeguarding data subjects and mitigating risks from an incident.

Records of risks and actions must be kept, so that the data protection duties can be undertaken at a suitable time. This may mean a delay in the normal statutory time frame of 72 hours for reporting to the ICO. This complies with Articles 33 and 34 of UK GDPR, and Section 67 and 68 of the DPA 2018 for personal data processed for law enforcement purposes.

If the incident may impact the processing of another party to this agreement, all relevant parties should be informed and appropriate coordination of the incident must take place. The decision to report the incident will lie with the data controller(s) of the information concerned. The parties agree to provide all reasonable and necessary assistance at their own expense to each other to facilitate the handling of any personal data breach in an expeditious and compliant manner.

It is confirmed that security breaches (including misuse or unauthorised disclosure) are covered by the partner's internal disciplinary procedures. If misuse is found there should be a mechanism to facilitate an investigation, including initiating criminal proceedings where necessary.

4.9 Retention & Disposal

Organisations are required by data protection legislation to document processing activities for personal data, such as what personal data is held, where it came from and with whom it has been shared. This Record of Processing Activity (ROPA) must include the retention period for the data.

Information must not be retained for longer than necessary for the purpose for which it was obtained. Disposal or deletion of personal data once it is no longer required, must be done securely with appropriate safeguards, in accordance with that organisation's disposal policies.

[3] https://www.gov.uk/government/publications/identifying-people-who-are-vulnerable-in-a-crisis-guidance-for-emergency-planners-and-responders.

5. Signatures

Most organisations will sign the agreement electronically via the Information Sharing Gateway.

[Signatures removed for public facing version of document].

……..

Version control	
Document production date	07th July 2022
Document version	Version 1.1. Public facing version of March 2022 (version 1.0) document.

6. Appendix A: Parties to this agreement

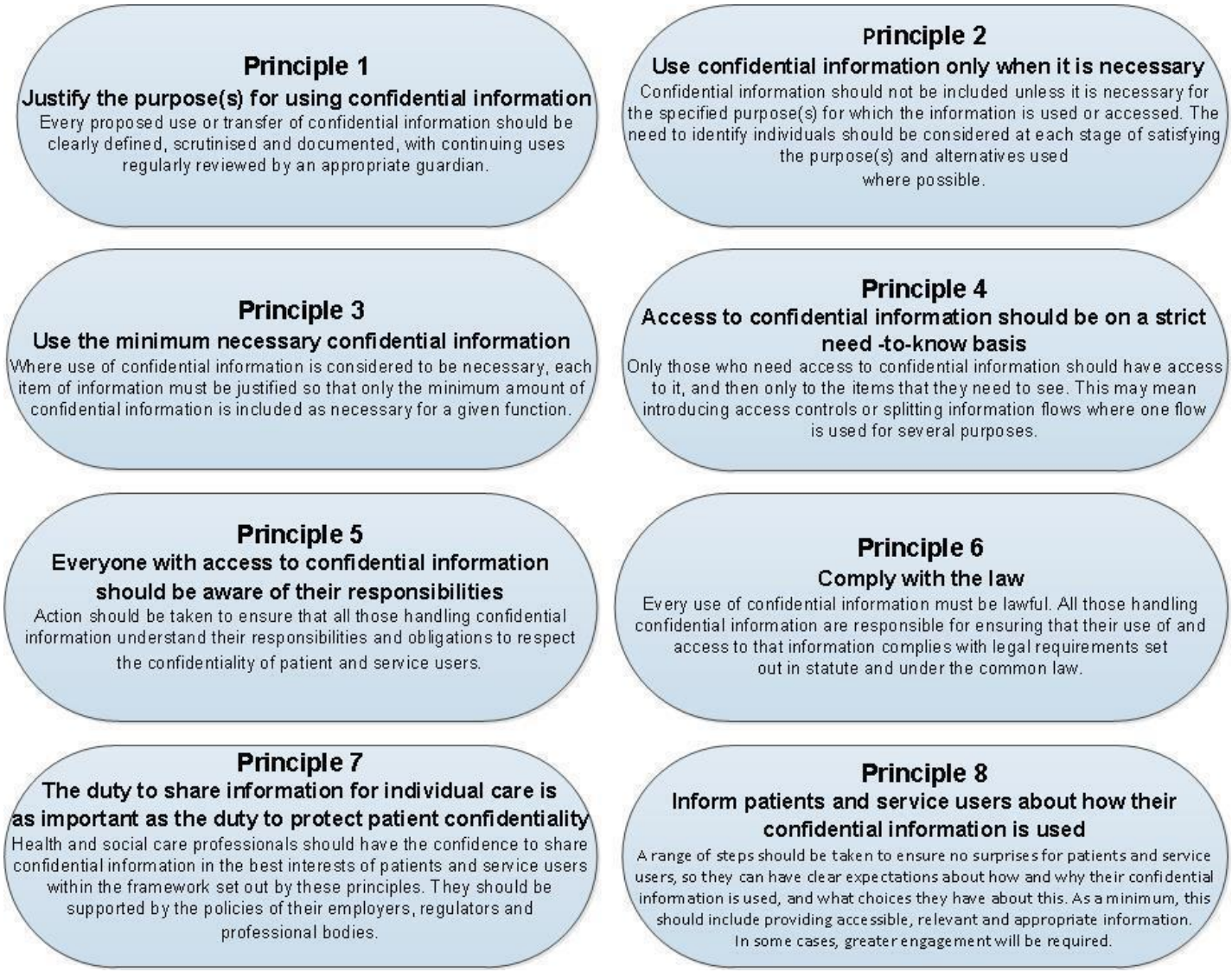
Responder	Organisation	Duties
Category 1	London Local Authorities	● Lead on humanitarian assistance provided to those individuals affected by emergency incidents. ● A suitable package of support for when those individuals return home, make potential arrangements for short- and long-term care, target their work appropriately (e.g. send educational psychologists to the right schools or make any adaptations to housing etc.) and fulfil their obligations to their local communities. ● Adult social care providers and community health care providers to work together to identify health and social care clients who are in community settings, including the location of patients/service users, what services they receive, and their level of need. ● Directors of Public Health to identify people who may have been exposed to a substance hazardous to their health in order to inform them about potential health implications. ● Provision of temporary or permanent housing during or following an incident. This may be carried out by a local authority's ALMO, or in conjunction with local housing associations.
Category 1	NHS England & NHS Improvement (London)	● Follow-up health care work or other support relevant to protecting them from physical, mental or emotional harm. ● Adult social care providers and community health care providers to work together to identify health and social care clients who are in community settings, including the location of patient's/service users, what services they receive, and their level of need.
Category 1	NHS Acute Trusts (x c.20)	● Follow-up health care work or other support relevant to protecting them from physical, mental or emotional harm. ● Adult social care providers and community health care providers to work together to identify health and social care clients who are in community settings, including the location of patient's/service users, what services they receive, and their level of need.
Category 1	NHS Mental Health Trusts (x10)	● Follow-up health care work or other support relevant to protecting them from physical, mental or emotional harm. ● Adult social care providers and community health care providers to work together to identify health and social care clients who are in community settings, including the location of patients/service users, what services they receive, and their level of need. ● Mental health screening services.

Responder	Organisation	Duties
Category 1	NHS Community Service Providers x4)	● Follow-up health care work or other support relevant to protecting them from physical, mental or emotional harm. ● Adult social care providers and community health care providers to work together to identify health and social care clients who are in community settings, including the location of patients/service users, what services they receive, and their level of need.
Category 1	UK Health Security Agency (HSA)	● To identify and follow up public health care on people who may have been exposed to infectious diseases, hazardous substances and other health threats.
Category 1	London Ambulance Service	● To share information about people they have treated with other organisations for the purpose of offering support services.
Category 1	Metropolitan Police Service	● To collate and share information appropriately to assist with: ● Survivors, Casualties, Deceased, Witnesses, Victims or Suspects involved or affected by an incident. ● Criminal investigations, or intelligence gathering. ● Safeguarding. ● Protection of life and property. ● Prevent the commission of offences. ● Maintain the Queen's Peace.
Category 1	British Transport Police	● As Metropolitan Police Service
Category 1	City of London Police	● As Metropolitan Police Service
Category 1	London Fire Brigade	● To share personal information about those involved in, or affected by, fire or other eventualities where doing so improves the safety, health or wellbeing outcomes for those people.
Category 2	Thames Water	● To share information about vulnerable customers with other organisations for the purpose of offering support services. ● To offer support services to vulnerable customers.
Other – Voluntary Sector	British Red Cross	● To support the practical and emotional needs of individuals affected by crises and emergency incidents.

7. Appendix B: Data Protection & Caldicott Principles

The Principles as described in Article 5 of the General Data Protection Regulation.

The Caldicott Principles



8. Appendix C: Applicable legislation and guidance

Legislation	Main purpose of Legislation
Civil Contingencies Act 2004[4]	The Civil Contingencies Act and accompanying non-legislative measures, delivers a single framework for civil protection in the UK. The Act is separated into 2 substantive parts: local arrangements for civil protection (Part 1); and emergency powers (Part 2).
HM Government 2021 Data Sharing in Emergency Preparedness, Response and Recovery. Non-statutory guidance on the sharing of Personal and Special Category Data during all phases of an emergency.	The purpose of this guidance is to inform organisations involved in the preparation for, response to, and recovery from emergencies on when they are able to lawfully share personal data under data protection legislation. This guidance supersedes and replaces the Data Protection and Sharing – Guidance for Emergency Planners and Responders (2007).[5]
The Mental Health Act 1983[6] and the Mental Health Act Code of Practice[7]	The Code of Practice provides statutory guidance to registered medical practitioners, approved clinicians, managers and staff of providers, and approved mental health professionals on how they should carry out functions under the Mental Health Act in practice. The act was substantially revised by the 2007 act but remains the key legislation. This regulation provides specific powers for dealing with mental health issues giving a legal basis under Section 8 of the DPA for this use. It specifically excludes learning disability, alcohol or drug dependence.
The Local Government Act 2000[8]	The main principles of the Local Government Act 2000 are to give powers to local authorities to promote economic, social and environmental well-being within their boundaries. This was mostly replaced by the Localism Act 2011 below, but still applies in Wales.
The Localism Act 2011[9]	The Localism Act created general powers for Local Government to act as an individual for any purpose, with specific goals to promote economic, social and environmental well-being within their boundaries. This regulation provides the general power for local authorities to act in any manner they believe suitable for the purposes giving a legal basis under Section 8 of the DPA for this use. However, as a general power it can be challenged, and an additional legal basis is preferred.
The Education Act 2002[10]	The Education Act 2002 puts a duty on schools to exercise their functions with a view to safeguarding and promoting the welfare of children. All schools are required by law to teach a broad and balanced curriculum which promotes the spiritual, moral and cultural development of pupils and prepares them for the opportunities, responsibilities and experiences of life.

[4] https://www.legislation.gov.uk/ukpga/2004/36/contents

[5] https://www.gov.uk/government/publications/data-protection-and-sharing-guidance-for-emergency-planners-and-responders

[6] https://www.legislation.gov.uk/ukpga/1983/20/contents

[7] https://www.gov.uk/government/publications/code-of-practice-mental-health-act-1983

[8] http://www.legislation.gov.uk/ukpga/2000/22/contents

[9] https://www.legislation.gov.uk/ukpga/2011/20/contents

[10] http://www.legislation.gov.uk/ukpga/2002/32/contents

	This regulation provides specific powers for dealing with school-related safeguarding and welfare issues giving a legal basis under Section 8 of the DPA for this use.
The Children Act 1989[11]	Under S.47 of the *Children's Act 1989*, a Local Authority has a duty to investigate when informed that a child in their area is in police protection or the subject of a protection order. This regulation provides specific powers giving a legal basis under Section 8 of the DPA for this use.
The Children Act 2004[12]	Under Sections 10 and 11 of the *Children Act 2004*, the police, local authorities and primary care trusts must co-operate with other relevant partners to safeguard and promote the welfare of children and ensure that arrangements are made to improve the wellbeing of children in their area. This regulation provides a general safeguarding and welfare power giving a legal basis under Section 8 of the DPA for this use
The Criminal Justice Act 2003[13]	This act amended a wide range of provisions in the PACE act and provided new regulations on offence management, disclosure and trials. The regulation clarifies process and procedure for police and their legal basis for use.
The Police and Criminal Evidence Act 1984[14]	This act makes the specific provision for the secretary of state to issue codes of practice to police with statutory effects. It provides the basis for many of the police actions in respect of matters relating to safeguarding and other matters, and as such provides their legal basis for use.
The Children & Social Work Act 2017[15]	The Children and Social Work Act 2017 (the Act) is intended to improve support for looked after children and care leavers, promote the welfare and safeguarding of children, and make provisions about the regulation of social workers. The Act sets out corporate parenting principles for the council as a whole to be the best parent it can be to children in its care. These are largely a collation of existing duties local authorities have towards looked after children and those leaving care.
The Mental Capacity Act 2005[16]	The Mental Capacity Act (MCA) 2005 promotes a person centred approach which promotes autonomy and for those who may lack mental capacity ensures that decisions made on their behalf are made in their best interests and with the least possible restriction of freedoms
The Health and Social Care Act 2012[17]	This act provides for the delivery of Health and Social Care, providing a legal basis for many of the services delivered by parties to this agreement. In particular, it places (section 251B) a duty to share information relating to health and adult social care unless the data subject has specifically objected. This regulation provides a specific duty giving a legal basis under Section 8 of the DPA for this use.

[11] https://www.legislation.gov.uk/ukpga/1989/41/contents
[12] https://www.legislation.gov.uk/ukpga/2004/31/contents
[13] http://www.legislation.gov.uk/ukpga/2003/44/contents
[14] https://www.legislation.gov.uk/ukpga/1984/60/contents
[15] http://www.legislation.gov.uk/ukpga/2017/16/contents
[16] http://www.legislation.gov.uk/ukpga/2005/9/contents
[17] https://www.legislation.gov.uk/ukpga/2012/7/contents

The Crime and Disorder Act 1998[18]	Each LA in England & Wales has the responsibility to formulate a strategy to reduce crime and disorder in their area and to work with police authorities to do this.
Care Act 2014[19]	The Care Act puts in place a framework for adult safeguarding and includes measures to guard against provider failure to ensure this is managed without disruption to services.
Housing Act 1996[20]	The Housing Act makes provision about housing, including provision about the social rented sector, houses in multiple occupation, landlord and tenant matters, the administration of housing benefit, the conduct of tenants, the allocation of housing accommodation by local housing authorities and homelessness; and for connected purposes.

[18] http://www.legislation.gov.uk/ukpga/1998/37/contents

[19] https://www.legislation.gov.uk/ukpga/2014/23/contents/enacted

[20] https://www.legislation.gov.uk/ukpga/1996/52/contents

9. Appendix D: Information Sharing Checklist

The following questions must be considered when deciding whether to share information.

- Whose information is this?
- Is there a lawful basis to share the information? Justify the purpose and identify relevant legislation that applies.
- Can information be pseudonymised or anonymised ahead of sharing?
- How have individuals been informed that the information will be shared e.g. via a privacy notice? Will they have the expectation that their information will be shared? Consider whether notifying the individual of the sharing may place someone at risk or prejudice a police or safeguarding investigation.
- Have any requests not to share been received and considered?
- How much information is it necessary to share in this situation?
- Is the information accurate and up to date? Has the difference between fact and opinion been stated?
- Is access to the information limited to only those who need it? Is it being given to the right person?
- Is the information being shared in a secure way?
- Has the decision to share or not share, and the rationale for the decision, been recorded?