

Information Sharing Agreement for the Leicestershire, Leicester and Rutland Local Resilience Forum

1. Partners/signatories

Category 1 Responders	Category 2 Responders
Leicestershire County Council Leicester City Council Rutland County Council Blaby District Council Charnwood Borough Council Harborough District Council Hinckley & Bosworth Borough Council Melton Borough Council North West Leics District Council Oadby& Wigston Borough Council University Hospitals Leicester NHS Trust Leicestershire Police Leicestershire Fire & Rescue Service East Midlands Ambulance Service Leicestershire Partnership NHS Trust Environment Agency Public Health England	Severn Trent Water National Grid East Midlands Airport Anglian Water Western Power

Version Number	Amendments Made	Authorisation	Date
0.1	Original draft by Kristie Marshman – Leicester City Council	n/a	29.09.15
1	Amendments by Ravi Nagra-Kumar – Leicestershire Police	Kristie Marshman	18.12.15

2. Introduction

The Civil Contingencies Act 2004 (CCA) is a legislative framework for civil protection in the United Kingdom. It places a statutory duty upon key responding and supporting agencies to prepare for and respond to emergencies.

Part 1 of the CCA and supporting Regulations and statutory guidance '[Emergency preparedness](#)' establish a clear set of roles and responsibilities for those involved in emergency preparation and response at the local level. The CCA divides local responders into 2 categories, imposing a different set of duties on each.

Category 1 Responders are organisations at the core of the response to most emergencies (the emergency services, local authorities, NHS bodies). Category 1 responders are subject to the full set of civil protection duties. They will be required to:

- Assess the risk of emergencies occurring and use this to inform contingency planning
- Put in place emergency plans
- Put in place business continuity management arrangements
- Put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform and advise the public in the event of an emergency
- Share information with other local responders to enhance co-ordination
- Co-operate with other local responders to enhance co-ordination and efficiency
- Provide advice and assistance to businesses and voluntary organisations about business continuity management (local authorities only)

Category 2 organisations (the Health and Safety Executive, transport and utility companies) are 'co-operating bodies'. They are less likely to be involved in the heart of planning work, but will be heavily involved in incidents that affect their own sector. Category 2 responders have a lesser set of duties - co-operating and sharing relevant information with other Category 1 and 2 responders.

Category 1 and 2 organisations will come together to form "Local Resilience Forums"(based on police areas) which will help co-ordination and co-operation between responders at local level. The Leicester, Leicestershire & Rutland Local Resilience Forum was created to meet this requirement.

3 Purpose - Why do you need to share this information?

This document is designed to assist LRF partner agencies to prepare for, and respond to a major incident regardless of cause at a tactical and/or strategic level.

In an emergency the sharing of personal information may be necessary to protect the affected person's vital interests. The information to be shared will be determined by the nature of the emergency. For example if there is a need to evacuate people from their homes, knowledge of where people with special needs are located would enable speedy application of appropriate assistance.

Sharing information is also necessary for responders to fulfil statutory functions and to perform public functions in the public interest in relation to the required response to emergency incidents (see related legislation and Guidance listed below). Additionally, in emergencies the sharing of personal information categorised as 'sensitive' is necessary.

In emergencies it may be in the interests of affected people who are most vulnerable for personal data to be shared with emergency responders. Sharing personal information will assist emergency responders to perform their statutory duties.

4 Legal Basis –What law allows you to share this information?

The Civil Contingencies Act 2004

The Civil Contingencies Act 2004 (CCA) part 1, as informed by related statutory and non-statutory Guidance including Emergency Preparedness (2005), Emergency Response and Recovery (2005), Data Protection and Sharing – Guidance for Emergency Planners and Responders (2007), Identifying People Who Are Vulnerable in a Crisis (2008).

Emergency Preparedness (2005) lists the duties placed on responders including the sharing of information with other local Category 1 and Category 2 Responders to enhance co-ordination, and the duty to co-operate with other local responders to enhance co-ordination and efficiency.

The Data Protection Act 1998 Schedule 2 list conditions, one or more of which must be met to allow the processing of non-sensitive personal information. Schedule 3 of the Act list further conditions, one or more of which must be met for the processing of sensitive personal information.

The Civil Contingencies Act 2004 part 1(1) defines an emergency as “an event or situation which threatens serious damage to human welfare and/or the environment, or war or terrorism which threatens serious damage to security”.

Guidance on Part 1 of the Civil Contingencies Act 2004 defines vulnerable people as those “that are less able to help themselves in the circumstances of an emergency”. Groups considered to be most vulnerable in emergencies include the following:

- a. children,
- b. older people,
- c. mobility impaired,
- d. mental/cognitive function impaired,
- e. sensory impaired,
- f. individuals supported by health or local authorities,

- g. temporarily or permanently ill,
- h. individuals cared for by relatives,
- i. homeless,
- j. pregnant women,
- k. minority language speakers,
- l. tourists,
- m. travelling community.

The principles and legislative provisions related to information sharing apply to the planning, response and recovery phases of emergencies.

Information sharing is only for the purposes of this agreement and the requirements of the Civil Contingencies Act 2004. Permission for any other ancillary use must be sought from the relevant data controller(s).

Statutory guidance sets out the responsibilities on Category 1 responders (with the co-operation of Category 2 responders) to plan for and meet the needs of those who may be vulnerable in emergencies. This includes:

- a. Making and maintaining plans for reducing, controlling or mitigating the effects of an emergency.
- b. Warning and informing.
- c. Business continuity.

Childrens Act 2004

Section 10 of the Children Act 2004 places a duty on Children's Services Authorities to make arrangements to promote co-operation between itself and relevant Partner agencies to improve the well-being of children in their area and for the police and other local authorities to co-operate in those arrangements.

Section 11 of the Children Act places a duty on local authorities and the police to make arrangements to ensure that their functions are discharged with regard to the need to safeguard and promote the welfare of children.

The Police Act 1996

The Police Act 1996 gives police constables certain powers. 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 any 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.

The Police also have a general common law power to disclose information for a policing purpose or purposes.

Local Government Act 2000

Section 2 of the Local Government Act 2000 as amended by the Localism Act 2011 enables local authorities to do anything to promote social, economic, or environmental well-being in their area provided that it is not specifically forbidden by other statute (including the Data Protection Act) and that in carrying out such activities they have regard to their sustainable community strategies.

In addition Section 111 of the Local Government Act 1972 enables local authorities to do anything conducive or incidental to the discharge of any of its functions

Data Protection Act 1998

The Data Protection provides a legal framework that guides organisations on how personal and sensitive information on citizens should be handled.

here are 8 key principles by which all organisations that are processing, storing or sharing personal information must adhere.

Of key importance to this sharing agreement are the conditions for processing under schedules 2 and 3.

Schedule 2 conditions met are;

- to comply with a legal obligation
- to protect the vital interests of the data subject
- for the exercise of certain functions of a public interest nature
- for the legitimate interests of the data controller unless outweighed by the interests of the data subject

Schedule 3 conditions met are;

- to protect the vital interests of the data subject or another person

Do we need to consider the Human Rights Act 1998?

Organisations can be directly challenged on action or inaction which leads to a breach of an individual's human rights.

Article 8: The right to respect for private and family life, home and correspondence. You may only interfere with the exercise of this right in accordance with the law and so far as is necessary in the interests of inter alia public safety and for the prevention of disorder or crime, or for the protection of health and morals. Individuals are entitled to enjoy the rights and freedoms set out in the Act without discrimination. Article 8 criteria met as follows;

- economic well-being of the country
- public safety
- protection of the rights and freedom of others

5 What Information may each signatory need to share?

- a. Name
- b. Address
- c. Postcode
- d. Telephone number
- e. Mobile phone number
- f. Date of birth
- g. Age
- h. Gender
- i. National Insurance Number
- j. National Health Number
- k. Religious affiliation
- l. Nationality
- m. Primary language
- n. Registered disability
- o. Mobility
- p. Support required
- q. Current known vulnerability
- r. Medical needs
- s. GP name and practice contact details
- t. Care/service providers
- u. Contact details of family members or significant others

NB. Always check whether the objective can still be achieved by passing less personal data.

6 How will the organisations decide who is the Data Controller?

The Chief Executive/Officer of the organisation which originally holds the information is the Data Controller.

For the purposes of this agreement, given the nature of the sharing which will be required in the event of an emergency, the data controller will change depending on the type of emergency response required. Below is brief explanation of the types of emergency situations and the resulting data controller responsibilities that could happen with the sharing of information under this agreement.

Example emergency situation resulting in organisations being Joint Data Controllers.

Identification of known vulnerable people in a localised power outage where we are looking to identify any clients who have a specific reliance on power - agencies could be local authorities, health, utility companies. In this scenario all partner organisations would be sharing information between them to solve the same issue.

Example emergency situation resulting in Data Controllers in Common.

Short – medium term evacuation (e.g.) discovery of an unexploded WWII bomb necessitating a planned evacuation. Same scenario as above but local authorities/health looking to identify vulnerable people to put appropriate measures in place whilst police/fire are looking to evacuate properties to secure the area. In this scenario the police could be utilising the same personal information but for a different purpose to the local authorities and health.

Example emergency situations resulting in a Data Processor.

Local authorities can provide mutual aid to others in the event of an emergency – this could see emergency test centre volunteers from one council supporting another council. In this scenario the local authority which is sending volunteers to help out would be a potentially a data processor only.

Where a partner is using individuals employed by another agency to process the information and deliver assistance the partner will accept responsibility for this processing and ensure that appropriate signed contracts or agreements are in place to ensure that the conditions contained within this ISA are adhered to by these other agencies. Please see Appendix B for the Confidentiality Agreement.

Providing Organisation	Receiving Organisation	Who is the Data Controller	Information to be shared	What will this be used for	Who will have access to this information

No data will be forwarded on to a third party or sub-contractor without the express written permission of the original data controller.

7 Indemnity

If parties are joint controllers or controllers in common, for the purpose of sharing during an emergency the following indemnity applies.

Each Party will keep each of the other Parties fully indemnified against any and all costs, expenses, claims and liabilities arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending Party or its sub-contractors, employees, agents or any other person within the control of the offending Party of any data obtained in connection with this agreement.

Except where any limitation is proscribed by law such as but not limited to death or personal injury resulting from negligence (for which there shall be no limit), the maximum total aggregate liability of either Party to the other Party for loss and damage under or in connection with this Agreement or its subject matter due to the

offending Party's breach, tort (including negligence), breach of statutory duty or otherwise howsoever arising shall not exceed five million UK pounds £5,000,000.00.

8 How are you going to keep information accurate?

Information will be for short term / emergency use only. Partners will ensure as far as possible that the information which they supply is accurate and where the receiving partners have difficulties matching that information with information already in their possession, will assist as far as possible to ensure that the correct information is data matched.

9 How long will the information be kept?

The Leicester Leicestershire and Rutland Resilience Forum will only use Personal Data provided for the purpose of any emergency. Partners to this agreement will delete personal data shared for the purpose of the emergency, once that emergency has been resolved.

10 How will we share and keep information secure?

LLR Prepared partner agencies to this agreement will not know what information is required, nor the means in which it will need to be shared until the emergency is clear and those partners who need to be involved have been contacted. In each emergency the following should be strictly adhered to but it is not possible at the point of writing this Agreement to outline how certain information will be shared and how that will be completed securely as this will change according to each emergency.

LLR Prepared partner agencies will abide by the security requirement of the Data Protection Act 1998 applicable to the processing of the information subject to this Agreement.

Partner organisations will make sure appropriate technical and organisational measures against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal information.

Every reasonable effort during an emergency situation will be made to:

- a. Deter accidental compromise or damage of data during storage, handling, and use, processing transmission or transport.
- b. Use only secure means of electronic transmission of information.
- c. Deter deliberate compromise or opportunist attack.
- d. Dispose of or destroy the data to ensure it cannot be reconstructed.
- e. Treat the data with the appropriate level of confidentiality and security.

Access to information subject to this Agreement will only be granted to those professionals who “need to know” in order to discharge their statutory duties effectively.

11 What if we want to use the information for something else?

If LLR Prepared partner agencies wish to use the information which they have been given under this agreement for any purpose other than that in Section 2 above, they must first ask the organisation which provided the information for their written consent.

12 What do we do if information is lost, disclosed, misused, etc?

If any information which is shared under this agreement is lost, stolen, or disclosed to someone who should not have seen it this is not only a breach of confidentiality but is likely to be a breach of the Data Protection Act (for which the Data Controller can be fined up to £500,000). If the information is deliberately accessed and/or disclosed by someone who is not entitled to see or use it this person may have committed a criminal offence under the Data Protection Act 1998 or the Computer Misuse Act 1990. Information may be deleted when it should have been kept. These are all information breaches.

It is important that the organisation(s) which provided the information are told as soon as possible so that they can risk assess what has happened – they may need to tell individuals what has happened to their information and they may need to tell the Information Commissioner. An investigation may have to be done by the police or the Information Commissioner so evidence (audit trails, printouts, etc) may need to be recovered.

The organisation where the breach occurred may need to do an internal investigation and this may lead to disciplinary action or identify processes which need to be changed.

Each organisation should provide contact details of the post in their organisation who should be informed if an information breach occurs in the table below.

Organisation	Post	Email	Telephone
Leicester City Council	Information Governance Manager	Info.requests@leicester.gov.uk	0116 4543100
Leicestershire County Council	Policy and Assurance Officer	Policyandassurance@leics.gov.uk	0116 305 8257
Rutland County Council	Head of Corporate Governance	dbaker@rutland.gcsx.gov.uk	01572 720941
Blaby District Council	Corporate Services Group Manager	Colin.jones@blaby.gov.uk	0116 272 7569

All partners have been consulted however signed agreements have not yet been received from all

Organisation	Post	Email	Telephone
Charnwood Borough Council	Strategic Director of Corporate Services	Simon.jackson@charnwood.gov.uk	01509 634699
Harborough District Council	Corporate Director	b.jolly@harborough.gov.uk	0185 8821 082
Hinckley & Bosworth Borough Council	Information Governance Officer	helen.rishworth@hinckley-bosworth.gov.uk	01455 255745
Melton Borough Council	Stewart Tiltman Corporate Governance Officer	stiltman@melton.gov.uk	01664 502432
North West Leicestershire District Council	Head of Legal and Support Services	Elizabeth.warhurst@nwleicestershire.gov.uk	01530 454 762
Oadby & Wigston Borough Council	PA to the Management Team Jo Smith	joanne.smith@oadby-wigston.gov.uk	0116 2572606
University Hospitals Leicester NHS Trust	Head of Privacy	Ewan.Robson@uhl-tr.nhs.uk	0116 258 8537
Leicestershire Police	Information Manager	Data.protection@leicestershire.pnn.police.uk	0116 248 5182
Leicestershire Fire & Rescue Service	Director of Service Support	andrew.brodie@lfrs.org	0116 229 2059
East Midlands Ambulance Service	Head of Information Governance	Janette.Kirk@emas.nhs.uk	0115 884 5127
Leicestershire Partnership Trust	Head of Information Governance	Sam.kirkland@leicspart.nhs.uk	0116 295 0997
Environmental Agency	Area Manager - Deputy Director - Derbyshire, Nottinghamshire and Leicestershire	lee.rawlinson@environment-agency.gov.uk	0203 0253 224
Public Health England			
Severn Trent Water	Security and Resilience Lead	GroupResilience@Severntrent.co.uk	Switchboard: 02477715000
National Grid			
East Midlands Airport	CISO	Peter.williams@magairports.com	01614893637
Anglian Water	Legal Compliance Officer	gbrittain@anglainwater.co.uk amorgan3@anglianwater.co.uk	01480326955
Western Power	Emergency Planning Officer	chenshaw@westernpower.co.uk	01332 827 683

13 How will you check if this agreement is being complied with and if it is still current?

You should all review this agreement after one year from signature so enter the date After this it should be reviewed every five years unless there has been some change (legislation, need to extend organisations involved, etc) which needs the agreement to be updated.

14 What happens if there is a major security breach?

Any organisation can suspend this ISA for 45 days if security has been seriously breached. This should be in writing and provide evidence of what went wrong. A representative from each organisation should meet asap (no longer than 14 days) to carry out a Risk Assessment and Resolution meeting.

Termination of this ISA should be in writing to all other Partner Organisations giving at least 30 days' notice

Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations 2004 (EIR)

Each partner organisation shall publish this Agreement on its website and refer to it within its publication scheme.

All recorded information held by public sector agencies is subject to the provisions of the FOIA or the EIR. Information requests made under the FOIA or the EIR will be co-ordinated and responded to by the organisation receiving the request in relation to the whole of the information held that is relevant to the request. Even where there is no requirement to consult with third parties in responding to requests for information, the parties to this ISA will consult the parties from whom information originated or relates to and will consider their views to inform the decision making process.

Nothing in this section shall prevent individual partner organisations from exercising their obligations and responsibilities under the FOIA or the EIR as they see fit.

16 Requests for Disclosure of Personal Information and Other Information Rights under the Data Protection Act 1998

Subject access requests and other notices relating to a data subjects rights made under the Data Protection Act 1998 will be co-ordinated and responded to by the organisation receiving the request and, where relevant, the fee. Even where there is no requirement to consult with third parties in responding to requests for information, the parties to this ISA will consult the parties from whom information originated or relates to and will consider their views to inform the decision making process.

Nothing in this section shall prevent individual partner organisations from exercising their obligations and responsibilities under the subject access provisions of the Data Protection Act 1998 as they see fit.

17 Amendments

If there are any key changes to this information sharing process, this agreement should be reviewed and updated

18 Who are the Responsible People in each organisation?

Each organisation should give details of the post which is responsible on a day to day basis for monitoring compliance with this ISA.

On behalf of Leicestershire County Council:

Post or Name: Fiona Holbourn
Address: County Hall, Leicester Road, Glenfield, LE3 8RA
Tel: 0116 305 6185
Email: fiona.holbourn@leics.gov.uk

On behalf of Leicester City Council:

Name: Martin Halse
Address: Leicester City Council, 2nd Floor Central Wing, City Hall, 115 Charles Street, Leicester LE1 1FZ
Tel: 0116 454 3621
Email: martin.halse@leicester.gov.uk

On behalf of Rutland County Council:

Name: Diane Baker
Address: Rutland County Council, Catmose, Oakham Rutland, LE15 6HP
Tel: 01572 720941
Email: dbaker@rutland.gcsx.gov.uk

On behalf of Blaby District Council:

Name: Colin Jones – Corporate Services Group Manager
Address: Blaby District Council, Council Offices, Desford Raod, Narborough, Leicester. LE19 2EP
Tel: 0116 272 7569
Email: colin.jones@blaby.gov.uk

On behalf of Charnwood Borough Council:

Name: Adrian Ward
Address: Council Offices, Southfields, Loughborough, Leicestershire, LE11 2TX
Tel: 01509 634573
Email: Adrian.ward@charnwood.gov.uk ;
Adrian.ward@charnwood.gcsx.gov.uk

On behalf of Harborough District Council:

Name: Stuart Done

Address: The Symington Building Adam & Eve Street Market Harborough
LE16 7AG
Tel: 01858 821164
Email: s.done@harborough.gov.uk

On behalf of Hinckley & Bosworth Borough Council:

Name: Helen Rishworth
Address: Hinckley Hub, Rugby Road, Hinckley, Leicestershire, LE10 0FR
Tel: 01455 255745
Email: helen.rishworth@hinckley-bosworth.gov.uk

On behalf of Melton Borough Council:

Name: Stewart Tiltman
Address: Parkside, Station Approach, Burton St, Melton Mowbray
LE13 1GH
Tel: 01664 502432
Email: stiltman@melton.gov.uk

On behalf of North West Leicestershire District Council:

Name: Mike Murphy
Address: Council Offices, Coalville, Leicestershire LE67 3FJ
Tel: 01530 454 4518 or 0777 194 6706
Email: mike.murphy@nwleicestershire.gov.uk

On behalf of Oadby & Wigston Borough Council:

Name: Jo Smith
Address: Council Offices, Station Road, Wigston, Leicester, LE18 2DR
Tel: 0116 2572606
Email: joanne.smith@oadby-wigston.gov.uk

On behalf of University Hospitals Leicester NHS Trust:

Name: Richard Mitchell
Address: Chief Operating Officer, Chief Executive's Department Level 3
Balmoral, Leicester Royal Infirmary, Infirmary Square, Leicester
LE1 5WW
Tel: 0116 2588569
Email: Richard.mitchell@uhl-tr.nhs.uk

On behalf of Leicestershire Police:

Name: XXXXXX
Address: XXXXXX
Tel: XXXXXX
Email: XXXXXXXX

On behalf of Leicestershire Fire & Rescue Service:

Name: Mick Grewcock
Address: Leicestershire Fire & Rescue Service, Service Headquarters
Geoff Monk Way, Birstall, LE4 3BU
Tel: 0116 229 2057
Email: mick.grewcock@lfrs.org

On behalf of East Midlands Ambulance Service:

Name: Janette Kirk
Address: East Midlands Ambulance Service NHS Trust, Notts Divisional
HQ, Beechdale Road, Nottingham, NG8 3LL
Tel: 0115 8845127
Email: Janette.kirk@emas.nhs.uk

On behalf of Leicestershire Partnership NHS Trust:

Name: Michael Ryan
Address: Leicestershire Partnership NHS Trust, Riverside House,
Thurmaston, Leicester
Tel: 0116 295 6567
Email: michael.ryan@leicspart.nhs.uk

On behalf of Environment Agency:

Name: Candice Sewell
Address: C/O Flood Resilience, Environment Agency, Scarrington Road,
West Bridgford, NG2 5FA
Tel: +442030253192
Email: Candice.Sewell@environment-agency.gov.uk

On behalf of Public Health England:

Name: **XXXXXX**
Address: **XXXXXX**
Tel: **XXXXXX**
Email: **XXXXXXXX**

On behalf of Severn Trent Water:

Name: Security and Resilience Lead
Address: Severn Trent Water Limited, Severn Trent Centre, 2 St John's
Street, Coventry, CV1 2LZ
Tel: 02477715000
Email: GroupResilience@severntrent.co.uk

On behalf of National Grid:

Name: XXXXXX
Address: XXXXXX
Tel: XXXXXX
Email: XXXXXXXX

On behalf of East Midlands Airport:

Name: Peter Williams
Address: Olympic House, Manchester Airport
Tel: 07766028815 or Via Service Desk (24 Hrs) 01614895005
Email: peter.williams@magairports.com

On behalf of Anglian Water

Name: Amy White
Address: Grafham WTW, Perry, Huntingdon, PE28 OBW
Tel: 07712876109
Email: awhite@anglianwater.co.uk

On behalf of Western Power:

Name: Carl Henshaw
Address: Western Power, Herald Way, Pegasus Business Park, Castle
Donington, DE74 2TU
Tel: 01332 827 683
Email: chenshaw@westernpower.co.uk

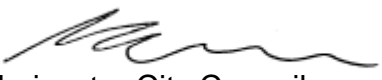
19 Signatories for the agreement of this ISA

Signed on behalf of Leicestershire County Council:

Name John Sinnott
Role Chief Executive
Signature 

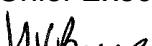
Organisation Leicestershire County Council
Date 03/06/16

Signed on behalf of Leicester City Council:

Name Miranda Cannon
Role Director of Delivery, Communications & Political Governance
Signature 


Organisation Leicester City Council
Date 10/02/16

Signed on behalf of Rutland County Council:

Name Helen Briggs
Role Chief Executive
Signature 


Organisation Rutland County Council
Date 26/02/16

Signed on behalf of Blaby District Council:

Name Colin Jones
Role Corporate Services Group Manager
Signature 


Organisation Blaby District Council
Date 23/05/16

Signed on behalf of Charnwood Borough Council:

Name Geoff Parker
Role Chief Executive
Signature 


Organisation Charnwood Borough Council
Date 06/04/16

Signed on behalf of Harborough District Council:

Name Norman Proudfoot
Role Corporate Director
Signature 


Organisation Harborough District Council
Date 10/02/16

Signed on behalf of Hinckley & Bosworth Borough Council:

Name Steve Atkinson
Role Chief Executive
Signature 


Organisation Hinckley & Bosworth Borough Council
Date 10/02/16

Signed on behalf of Melton Borough Council:

Name Lynn Aisbett
Role Chief Executive
Signature 


Organisation Melton Borough Council
Date 01/03/16

Signed on behalf of North West Leicestershire District Council:

Name Mike Murphy
Role HR Manager
Signature 


Organisation North West Leicestershire DC
Date 08/06/16

Signed on behalf of Oadby & Wigston Borough Council:

Name Mark Hall
Role Chief Executive
Signature 


Organisation Oadby & Wigston Borough Council
Date 17/03/16

Signed on behalf of University Hospitals Leicester NHS Trust:


Name Andrew Furlong
Role Medical Director
Signature 

Organisation University Hospitals Leicester NHS Trust
Date 19/02/16


Signed on behalf of Leicestershire Police:

Name Simon Cole
Role C.C.331
Signature 
Organisation Leicestershire Police
Date 31/05/16


Signed on behalf of Leicestershire Fire & Rescue Service:

Name Steve Lunn
Role Chief Fire Officer/Chief Executive Officer
Signature 
Organisation Leicestershire Fire & Rescue Service
Date 01/06/16


Signed on behalf of East Midlands Ambulance Service:

Name Bob Winter
Role Medical Director
Signature 
Organisation East Midlands Ambulance Service
Date 04/12/16

Signed on behalf of Leicestershire Partnership NHS Trust:

Name Dr. Satheesh Kumar
Role ~~Medical Director~~ **Caldicott Guardian**
Signature 
Organisation Leicestershire Partnership NHS Trust
Date 22/02/16


Signed on behalf of Environment Agency:

Name Lee Rawlinson
Role Area Manager
Signature 
Organisation Environment Agency
Date 12/02/16

Signed on behalf of Public Health England:

Name _____
Role _____
Signature _____
Organisation _____
Date _____

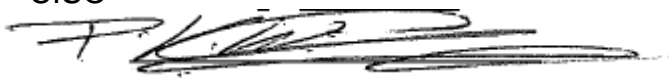
Signed on behalf of Severn Trent Water:

Name Sam Harris
Role Resilience Specialist
Signature 
Organisation Severn Trent Water
Date 16/06/16

Signed on behalf of National Grid:

Name _____
Role _____
Signature _____
Organisation _____
Date _____

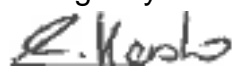
Signed on behalf of East Midlands Airport:

Name Peter Williams
Role CISO
Signature 
Organisation Airport
Date 19/04/16

Signed on behalf of Anglian Water:

Name Amy White
Role Emergency Planning Manager
Signature _____
Organisation Anglian Water
Date 03/03/16

Signed on behalf of Western Power:

Name Carl Henshaw
Role Emergency Planning Officer
Signature 
Organisation Western Power
Date 01/04/16

First Principle

First Principle Requirements of Lawfully and Fairly	How will partners satisfy these requirements?
<p>DUTY OF CONFIDENCE Confidentiality arising from the relationship of the data controller with the data subject. This provision restricts the data controller from using the information for a purpose other than that for which it was provided.</p>	<p>All partners to this agreement will have notified the Information Commissioner of their holding data under a relevant purpose. All disclosures within this agreement will be for this purpose.</p> <p>Partners will proactively communicate to individuals and the community at large that this sharing takes place and will deal with any specific requests for information not to be shared on a case by case basis.</p>
<p>ULTRA VIRES RULE The ultra vires rule and the rule relating to the excess of delegated powers under which the data controller may only act within the limits of its legal powers.</p>	<p>The partners are relying upon the legislation in Section 3 to provide the vires to share information with the parties to this agreement.</p>
<p>LEGITIMATE EXPECTATION Legitimate expectation, that is, the expectation of the individual as to how the data controller will use the information relating to him.</p>	<p>It is argued that where an individual is the subject of any of the sharing activities listed in this agreement, that individual must reasonably expect that agencies involved with supporting the law enforcement function or other relevant functions will share information required to effectively undertake those functions.</p> <p>Partners will proactively communicate to individuals and the community at large that this sharing takes place.</p>
<p>ARTICLES HUMAN RIGHTS Article 8 of the European Convention on Human Rights (the right to respect for private and family life, home and correspondence). There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".</p>	<p>The purposes for which the defined datasets are being shared will always satisfy one of more these conditions in particular the sharing of information will contribute to promoting economic well-being, and protecting of the rights and freedoms of others and public safety.</p>

<p>FAIR PROCESSING When data are obtained from data subjects the data controller must ensure, so far as practicable that the data subjects have, are provided with, or have made readily available to them, the following information :- (a) the identity of the data controller (b) if the data controller has nominated a representative for the purposes of the Act, the identity of that representative (c) the purpose or purposes for which the data are intended to be processed (d) any further information which is necessary taking into account the Specific circumstances in which the data are or are to be processed to enable processing in respect of the data subject to be fair.</p>	<p>Partners will proactively communicate to individuals and the community at large that this sharing takes place.</p>
<p>First Principle Requirements to satisfy conditions in Schedule 2 Data Protection Act 1998</p>	<p>How will partners satisfy these requirements? Note: Only one of the conditions needs to apply</p>
<p>CONSENT</p>	<p>It will not be possible to gather consent as the sharing of information will be done under emergency situations.</p>
<p>LEGAL OBLIGATION The processing is necessary to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.</p>	<p>Section 3 of this agreement sets out the relevant legal obligations which are exercisable by partners in support of the objectives of the programme set out in section 1.</p>
<p>EXERCISING LEGAL FUNCTIONS - 1 The processing is necessary for the exercise of any functions conferred by or under any enactment.</p>	<p>Section 3 of this agreement sets out the relevant legal functions which are exercisable by partners in support of the objectives of the programme set out in section 1.</p>
<p>LEGITIMATE INTERESTS The processing is necessary for the purpose of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed.....</p>	<p>Section 2 of this agreement sets out the relevant legitimate interests which are exercisable by partners in support of the objectives of the programme .</p>
<p>PUBLIC FUNCTIONS For the exercise of any other functions of a public nature exercised in the public interest.</p>	<p>Section 3 of this agreement sets out the relevant legal functions which are exercisable by partners in support of the objectives of the programme set out in section 2.</p>

First Principle Requirements to satisfy conditions in Schedule 3 Data Protection Act 1998	How will partners satisfy these requirements? Note: Only one of the conditions needs to apply
IMPLICIT CONSENT	It will not be possible to gather consent as the sharing of information will be done under emergency situations.
ADMINISTRATION OF JUSTICE or EXERCISE OF A FUNCTION 7 (1) the processing is necessary - (a) for the administration of justice, (b) for the exercise of any functions conferred on any person by or under an enactment.	Section 3 of this agreement sets out the relevant legal functions which are exercisable by partners in support of the objectives of the programme set out in section 2.
Data Protection (Processing of Sensitive Personal Data) Order SI 2000 No 417 1 (1) The processing – (a) is in the substantial public interest; (b) is necessary for the purposes of the prevention or detection of any unlawful act; and (c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.	Processing will only be undertaken in circumstances where it is “in the substantial public interest” e.g. in order to protect public safety and vulnerable people in an emergency situation.
Data Protection (Processing of Sensitive Personal Data) Order SI 2000 No 417 (4) “The processing – (a) is in the substantial public interest; (b) is necessary for the discharge of any function which is designed for the provision of confidential counselling, advice, support or any other service; and (c) is carried out without the explicit consent of the data subject because the processing – (i) is necessary in a case where consent cannot be given by the data subject, (ii) is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of the data subject, or (iii) must necessarily be carried out without the explicit consent of the data	Processing will only be undertaken in circumstances where it is “in the substantial public interest” e.g. in order to protect public safety and vulnerable people in an emergency situation.

subject being sought so as not to prejudice the provision of that counselling, advice, support or other service.	
Data Protection (Processing of Sensitive Personal Data) Order SI 2000 No 417 (10) The Processing is necessary for the exercise of any functions conferred on a constable by any rule of law	Processing will only be undertaken in order to protect public safety and vulnerable in an emergency situation.

Second Principle

Second Principle Requirements	How will partners satisfy these requirements?
Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner Incompatible with that purpose or those purposes.	The information is being shared to identify people and families who need help and assistance in emergency situations.

Third Principle

Third Principle Requirements	How will partners satisfy these requirements?
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	Because the purposes specified are wide ranging it is not possible to be prescriptive in relation to individual data fields, forms and printouts. However, partners to this agreement will comply with this principle by only disclosing to each other what is needed to achieve the purpose.

Fourth Principle

Fourth Principle Requirements	How will partners satisfy these requirements?
Personal data shall be accurate and, where necessary, kept up to date	Partners will take all necessary precautions to ensure that information at the time of the emergency is accurate and up to date.

Fifth Principle

Fifth Principle Requirements	How will partners satisfy these requirements?
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.	Data will only be kept after the emergency by the Leicestershire, Leicester and Rutland Resilience Forum for the purpose of any potential inquiry or investigation processes.

Sixth Principle

Sixth Principle Requirements	How will partners satisfy these requirements?
<p>Personal data shall be processed in accordance with the rights of data subjects under this Act.</p>	<p>Partners to this agreement will respond to any notices from the Information Commissioner that impose requirements to cease or change the way in which data is processed. In the event that a subject access request is received by a partner and personal data provided by another partner is identified, the partners will liaise and assess whether an exemption (potentially under Section 29) of the Data Protection Act, 1998 is appropriate.</p>

Seventh Principle

Seventh Principle Requirements	How will partners satisfy these requirements?
<p>Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.</p>	<p>Partners to this agreement will abide by the security requirement of the Data Protection Act 1998 applicable to the processing of the information subject to this Agreement.</p> <p>Partner organisations will make sure appropriate technical and organisational measures against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal information.</p>

Eighth Principle

Eighth Principle Requirements	How will partners satisfy these requirements?
<p>Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.</p>	<p>Since this is a local agreement this section will not be relevant.</p>

Appendix A

Sharing & Destruction Methods	Security Requirements
Organisation Data Network (e.g. internal email)	<p>Recommend passwording attachments for sensitive personal data in case it is sent to wrong email address. No personal data in subject title, or sensitive personal data in body of email. Use of GCSx network where available.</p> <p>Recommend turning off autofill of address field.</p>
Email between partners	<p>Passwording attachments for sensitive personal data in case it is sent to wrong email address. No personal data in subject title, or sensitive personal data in body of email</p> <p>To/from Police: Restricted or sensitive personal data only to emails using PNN, GSI, CJSM or MOD secure addressing conventions or via GCSx and PSN connections.</p> <p>To/From NHS: Secure transfer as agreed with health partners (currently under discussion county-wide due to new health arrangements - To be updated when agreed).</p>
Laptops, removable media, USB, etc	<p>Must be owned by the employer and encrypted. No personal information from any of the organisations in this ISA is to be loaded to personally owned removable media.</p>
Electronic storage of information	<p>Has the application where it will be stored been pen tested? In other words, could someone hack into it? Check with your IT department.</p> <p>How will access to the information be restricted. Please say how this will be done</p> <p>Is there an audit trail which will show who has accessed a record.</p>
Vetting/clearance of staff	<p>Have the staff who will receive and access the information been vetted.</p>
Internal and public telephone network	<p>May be used.</p>
Mobile telephone (voice and text)	<p>Digital cell phones may be used.</p> <p>Only use analogue cell phones if operationally</p>

	urgent, use guarded speech and keep conversation brief.
Fax	Note faxes are legacy technology and are NOT to be used unless there is no alternative. If no alternative, check recipient is on hand to receive. Send cover sheet first and wait for confirmation before sending. Request confirmation that the fax has been received.
Storage of papers	Protected by one barrier, e.g. a locked container within a secure building/room. Locked filing cabinet for storage if home working.
Disposal of papers	Use secure waste sacks if organisation has system in place and make sure they are secure when left unattended or collected for destruction. Shred personal information if it is very sensitive.
Disposal of magnetic media	All types of discs and other storage devices – dismantle and destroy by disintegrating, pulverising, melting or shredding then dispose with normal waste/recycling following destruction.
Movement within organisation via internal mail	In a sealed envelope with protective marking shown.
Movement between partner agencies	By post or courier in a sealed envelope.
Movement between workplace and home / mobile office	On encrypted memory stick or lockable briefcase. Locked filing cabinet for storage if home working.

* If organisations do not find it possible to apply the appropriate security this should be discussed with the originator.

APPENDIX B - CONFIDENTIALITY STATEMENT

To enable the exchange of information between attendees at this emergency to be carried out in accordance with the Data Protection Act 1998, the Human Rights Act 1998 and the common law duty of confidentiality, all organisations not signed up the sharing agreement are asked to agree to the following. This agreement will be stored by the Leicester, Leicestershire and Rutland Resilience Forum.

1. Information can be exchanged during this emergency for the purpose of identifying any action that can be taken by any of the agencies or departments to resolve the problem.
2. A disclosure of information outside the partner organisations taking part in the emergency, beyond that agreed, will be considered a breach of the subjects' confidentiality and a breach of the confidentiality of the agencies involved.
3. All minutes, documents and notes of disclosed information should be kept in a secure location to prevent unauthorised access.
4. If further action is identified, the agency(ies) who will proceed with this action(s) should then make formal requests to any other agencies holding such personal information as may be required to progress this action quoting their legal basis for requesting such information.

This confidentiality agreement is in relation to the

Emergency.....

Signature.....Date.....

Name.....

Representing...(Name and/or Organisation)

.....

Copies of this signed agreement are to be held by the Local Resilience Forum.

All partners have been consulted however signed agreements have not yet been received from all

Notes

*For North West Leicestershire District Council, in an emergency situation the data controller will be the on-call Incident Control Officer.