INFORMATION SHARING AGREEMENT

For the purposes of Emergency Planning, Exercising, Response and Recovery

BETWEEN THE MEMBERS OF LINCOLNSHIRE'S RESILIENCE FORUM (and organisations to support them in their objectives)

Lincolnshire's Resilience Forum

PREPARING FOR EMERGENCIES
WHAT YOU NEED TO KNOW

CONTENTS

SUMMARY SHEET

Title of Agreement	Information Sharing Agreement for Lincolnshire's Resilience Forum
Agreement Reference	
Purpose	To facilitate the sharing of information between the organisations of Lincolnshire's Resilience Forum to ensure all partners understand their roles and responsibilities for sharing information for the purposes of Emergency Planning and Response.
Partners	As per Section 6
Date Agreement comes into force	1 October 2015
Date of Agreement review	April 2016
Agreement owner	Lincolnshire Resilience Forum Secretariat
Agreement drawn up by:	Lincolnshire County Council Emergency Planning and Business Continuity Service on behalf of Lincolnshire's LRF
Location of Agreement in force	Resilience Direct

VERSION RECORD

Version Number	Amendments Made	Authorisation
1	New agreement	PMB

1. INTRODUCTION

1.1 This Information Sharing Agreement has been drawn up to assist the organisations involved in Lincolnshire's Resilience Forum to share information, as specified in the Civil Contingencies Act (2004), in a safe and secure manner.

1.2 This agreement covers only the data and information required to plan for and respond to emergencies This includes data and information shared for use during the testing and exercising of emergency planning.

1.3 The Lincolnshire Resilience Forum is a number of organisations that come together to respond to emergencies. It needs to be noted that this agreement is not between individual organisations and the Local Resilience Forum (LRF), as the LRF is not a legal entity. This agreement is between individual organisations and exists to set out the principles of good information sharing and minimal security standards for data exchange and management.

1.4 Some organisations that are signed up to this agreement are not members of the LRF but, as associated organisations, have been added into this agreement as it is reasonable to foresee that information will need to be shared with them.

1.5 In all circumstances it will be essential that information is handled and exchanged securely and each organisation must ensure that the appropriate legal pathway for this is defined and followed. All activities in relation to information sharing will be subject to audit.

1.6 Listed below are the definitions of a number of key terms and phrases used throughout this information sharing Agreement:

"**Agreement**" means this Information Sharing Agreement

"Category 1 and 2 responder" are defined under the Civil Contingencies Act 2004, and have duties placed on them accordingly. Further information is available in section 2 of this Agreement.

"**Data Controller**" has the meaning defined in the Data Protection Act 1998 which "a person who (either alone or jointly in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed".

"**Data Subject**" means the individual who is the subject of the information.

"Emergency planning, exercising, response and recovery" are the activities undertaken in preparing for any emergencies that may occur in Lincolnshire.

"**Information Sharing Lead**" means the individual with responsibility for overseeing the sharing of information within each Partner organisation.

"**Originating Organisation**" means the organisation that discloses information to another organisation.

"**Partner**" means any organisation that is listed as a party to this Agreement

"**Recipient Organisation**" means the organisation to which information is disclosed.

"Sensitive information" is also defined as: information that is not reasonably accessible to the public because its disclosure to the public would, or would be likely to

a) Adversely affect national security
b) Adversely affect public safety
c) Prejudice the commercial interest of any person, or information that is personal data, within the meaning of section 1(1) of the Data Protection Act 1998, disclosure of which would breach that Act.

2. POLICY STATEMENTS AND PURPOSE

2.1 The purpose of this document is to facilitate an agreement between Category 1 and 2 responders (under the Civil Contingencies Act (2004)) in respect to the exchange of information in the planning, exercising, response and recovery to an emergency.

2.2 Compulsory duties under the Civil Contingencies Act (2004) to Category 1 responders (organisations) that are involved with emergency planning and response are as follows:

- To conduct emergency planning
- Undertake risk assessments
- Create Business Continuity Plans
- Co-operate with other responders
- Information Sharing
- Warn and Inform the public (of risks)

2.3 In addition to these 6 compulsory duties, Local Authorities are also charged with promoting business continuity to small and medium businesses and the voluntary sector. Category 2 responders are obliged to co-operate and share information with other agencies: including Category 1 and 2 organisations. A breakdown of Category 1 and Category 2 responders is shown in the table below.

Category 1 Responders	**Category 2 Responders**
Local Authorities (County and District/Borough/City)	Utility Providers
Emergency Services	Transport Companies
Health Community	Health and Safety Executive
Port Health Authority	Public Communication Providers
Environment Agency	Port and Harbour Authorities
	Network Rail
	Airport Operators

2.4 The information provided may include personal and sensitive information, GIS mapping data sets, CCTV imagery, specific risk information, infrastructure assets, contents of emergency plans and response data following incidents. The information that could be asked for cannot be defined in this agreement as it will be dependent on the nature of the incident, exercise or planning process being undertaken. However the principles of this agreement should apply under all circumstances.

2.5 It needs to be noted that organisations belonging to the LRF may have information sharing agreements in place with organisations outside Category 1 and 2 responders that may also fit in with emergency planning and response activities. If it is intended for the information shared to be used for emergency planning or response purposes and shared in a wider partnership setting this should be stated when requesting the information so it can be taken into consideration by the organisation providing the data.

2.6 There may be circumstance when on-going information may be shared with organisations to support LRF with its objectives. This may include a variety of partner organisations. Information shared between the Partners to this agreement may be shared with third party organisations within the LRF on a need to know basis. Information shared with third parties shall be strictly in accordance with the purpose set out in this Agreement and only the minimum information required to fulfil that purpose will be shared. Third party recipients will be advised that use of any information shared with them for the purpose of this agreement is strictly restricted. Each Partner who shares information with a third party is solely responsible for ensuring that the sharing of such information is lawful and in accordance with the terms set out in this agreement.

2.7 Examples of other organisations include:

- St Barnabas Hospice
- Private adult care providers
- Tele-care providers
- Internal Drainage Boards
- Voluntary Sector organisations

3. PARTNERS

3.1 This Agreement is between the organisations identified in Annex B.

3.2 Other partners not identified in Annex B may assist the LRF with emergency planning, exercising, response and recovery. Where this is done, the principles of this agreement will still apply.

3.3 The majority of partners identified belong to the LRF. There have been complementary partners added to this agreement where it is reasonably foreseeable that information may be requested from them. These organisations do not have duties under the Civil Contingencies Act 2004, but have consented to be a signatory to this agreement.

3.4 If a new Partner joins the Agreement, a new version of the Agreement will be issued as soon as possible and circulated to all participating parties.

3.5 If a Partner leaves the Agreement, a new version of the Agreement will be issued as soon as possible to all participating parties. Partners must refer to section 5.8 regarding retention and deletion of information that has been shared.

4. BASIS FOR SHARING

4.1 This Agreement fulfils the requirements of the following;

- The Data Protection Act 1998 (Principle 1) Schedules 2 and 3
- The Human Rights Act 1998 (Article 8)
- The Freedom of Information Act 2000
- Civil Contingencies Act 2004
- Common Law Duty of Confidentiality
- Local Government Act
- The Children Act 1989
- The Children Act 2004
- Care Act 2014

4.2 Any information shared and the processes used to share such information will be compliant with the relevant Human Rights legislation.

4.3 Under the Civil Contingencies Act 2004, organisations designated as Category 1 or Category 2, have a legal responsibility to share information.

4.4 There is a Memorandum of Understanding (MoU) between Lincolnshire County Council and the voluntary sector. Information sharing under the MoU will take the principles of this Information Sharing Agreement into account.

4.5 The principles of information sharing for this agreement should be applied as follows:

- Data protection legislation does not prohibit the collection and sharing of personal data – it provides a framework where personal data can be used with confidence that individuals' privacy rights are respected.
- Emergency responders' starting point should be to consider the risks and the potential harm that may arise if they do not share information.
- Emergency responders should balance the potential damage to the individual (and where appropriate the public interest of keeping the information confidential) against the public interest in sharing the information.
- In emergencies, the public interest consideration will generally be more significant than during day-to-day business.
- Always check whether the objective can still be achieved by passing less personal data.
- The consent of the data subject is not always a necessary pre-condition to lawful data sharing. Even without explicit consent for the sharing of sensitive personal data, it is still possible to share the data legitimately if this is necessary in order to exercise any statutory function (as may well be the case for responders) or to protect the vital interests of the individual where, for example, consent cannot be given.

5. PROCESS

5.1 This Agreement has been formulated to facilitate the exchange of information relevant to emergency planning and response between the Partners listed. It is, however, incumbent on all Partners to recognise that any information shared must be justified on the merits of the Agreement. The balance, between an individual's Human Rights and the need to disclose information, must be assessed to ensure the information shared between agencies is proportionate to the purpose. Anyone in doubt should consult their Information Sharing Lead before proceeding.

It is acknowledged that for the purposes of this agreement ad hoc rather than routine information may be required. This is determinate on the data required to inform good emergency planning.

5.2 INFORMATION TO BE SHARED

5.2.1 Information that is shared should be labelled with the name of its originator, so that obligations regarding withdrawal of consent, maintenance of accurate records and reporting any breaches can be fulfilled.

5.2.2 If there is a need to share additional information on a one-off-basis, the Partners concerned should consider whether the sharing is necessary to the Agreement and document their considerations/findings, including any additional consents sought (and if not sought, an explanation as to why).

5.2.3 If additional information is required on a repeated basis over and above what is defined in this Agreement, to enable the Agreement to achieve its aims, the Information Sharing Leads should agree an addition to the Agreement, ensuring that the new information meets the same legislative or consent basis as the original. This addition should be added to the Agreement and all parties should sign up to the amended Agreement.

5.2.4 Information will be shared through Resilience Direct – the Cabinet Office information sharing platform for emergency planning and response to which all Lincolnshire's LRF partners have agreed to use for the speedy dissemination of live incident data and information for planning purposes. For those organisations signed up to this agreement who are not members of the LRF, access to information should be sought through LCC Emergency Planning and Business Continuity Service.

5.3 CONSENT

5.3.1 Any request for the sharing of information needs to be made in writing (hard copy or email) to the SPOC within the organisation being asked for the information.

5.3.2 When the request is being made, the following information will be included:

- Date of request
- Details of the information required and what it will be used for
- Details of the requestor
- Summary of information provided
- Grounds for sharing

5.3.3 The information should be provided, unless the information is sensitive and disclosure would have adverse effects. If necessary, obtaining consent to disclosure from a body which deals with security matters. Non-disclosure should be limited to exceptional circumstances and information only part of which is sensitive should be shared with the sensitive parts removed.

5.3.4 During an emergency, it may be that personal information needs to be shared without formal consent to protect an individual's vital interests. The information to be requested and/or 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 particular vulnerabilities are located would enable speedy application of appropriate assistance.

5.3.5 Sharing information is also necessary for responders to fulfil statutory functions and to perform public safety functions during emergency response.

5.3.6 Where the sharing of personal information is necessary to protect a person's vital interests, the information should only be shared on a 'need to know' basis to support a positive outcome.

5.3.7 It is recognised that some information may be subject to receiving officers undertaking security checks as documentation may be marked under the Government Security Classification scheme. It is the responsibility of all organisations to ensure that information is only requested and sent to those with valid security checks where documents are marked 'official', 'secret' or 'top secret'.

5.3.8 There may be additions to this, such as 'Official – Sensitive' or 'Official – LRF use only'. These indicate that the information must only be granted on the basis of a genuine 'need to know' and appropriate personnel security control.

5.3.9 As such, some organisations party to this agreement may not have adopted the scheme, but may work to its principles. Where clarification is sought, this should be done prior to information being shared.

5.4 RIGHT TO SHARE ANONYMISED AND PSEUDONYMISED INFORMATION

5.4.1 Periodically, organisations signed up to this agreement will undertake exercises designed to test their capability to respond to an emergency situation. Where information is requested as part of this, it should be anonymised where possible.

5.4.2 Any requests for information resulting from an exercise should be saved, marked with the exercise name and the date it took place.

5.5 MINIMUM INFORMATION SECURITY STANDARDS

5.5.1 Annex A provides the minimum information security standards required of participating organisations to manage the information they receive from other parties under this Agreement. These principles must be respected by all signatories.

5.5.2 Information will be shared by a secure method, for example secure email (GCSX, PNN, NHSNET) or through Resilience Direct information sharing portal for the SPOC's and deputies). Where secure email does not already exist, a representative from Lincolnshire County Council can email any recipient first and create a secure email link using LCC Secure Mail.

5.6 ENSURING DATA QUALITY

5.6.1 Each Partner sharing data under this Agreement is responsible for the quality of the data it is sharing.

5.6.2 Before sharing data, officers will check that the information being shared is accurate and up to date to the best of their knowledge. If sensitive data is being shared which could harm the data subject if it was inaccurate, then particular care must be taken.

5.6.3 Where a 'dataset' is being shared (i.e. structured data), it will be accompanied by a table providing definitions of the data fields if one is available.

5.6.4 If a complaint is received from a Partner about the accuracy of personal data which affects data shared with Partners in this Agreement, an updated replacement document will be communicated to the Partners. The Partners will replace the out of date data with the revised data.

5.7 SUBJECT ACCESS REQUESTS AND COMPLAINTS

5.7.1 Subject Access is an individual's right to have a copy of information relating to them which is processed by an organisation.

5.7.2 Once information is disclosed from one agency to another, the recipient organisation becomes the Data Controller for that information. With regards to subject access requests, the Data Controller has a statutory duty to comply with Section 7 of the Data Protection Act, unless an exemption applies. It is good practise for the recipient organisation to contact the originating organisation. This enables the originating organisation to advise the use of any statutory exemptions that may need to be applied prior to disclosure to the requesting individual. Communication should take place speedily thus allowing the servicing of the request to take place within the Statutory 40 calendar day time period.

5.7.3 Complaints made by Data Subjects involving a breach of this Agreement should be dealt with by utilising any established policies and procedures for breaches and complaints made in relation to appropriate legislation in connection with the agreed information exchange and data processing by the Partner receiving the complaint.

5.7.4 Any disclosure of information by an employee, which is done in bad faith or for motives for personal gain, will be the subject of an investigation and be treated as a serious matter. Each Partner will be accountable for any misuse of the information supplied to it and the consequences of such misuse by its employees, servants or agents.

5.7.5 All Partners are reminded of the Data Protection Act Principles and Section 55 and Section 61 Offences.

5.7.6 It is the responsibility of all Partners to notify each other of any known breach or infringement immediately and remedial action must be agreed and actioned by all relevant Partners concerned.

5.7.7 Major breaches may result in this agreement being temporarily suspended or withdrawn completely.

5.8 INFORMATION USE, REVIEW, RETENTION AND DELETION

5.8.1 Partners to this Agreement undertake that information shared under the Agreement will only be used for the specific purpose for which it was shared, in line with this Agreement. It must not be shared for any other purpose outside of this Agreement.

5.8.2 As party to this agreement, all Partners will become joint Data Controllers where information is shared through LRF mechanisms. Where information is edited by the receiver, they must make it clear this is an altered copy.

5.8.2 The retention period for the information shared should be agreed and documented between partners sharing the information prior to sending/receiving.

5.8.3 The recipient will not release the information to any third party without obtaining the express written authority of the Partner who provided the information unless it is under a legal obligation to do so

5.8.4 Records, whether electronic or hard copies should be disposed of using the records destruction policy of the receiving organisation, following expiration of the retention period. Records destruction policies should be available on organisation's websites or readily available. All records on Resilience Direct will be deleted from the system at a time agreed between the requesting and providing organisation.

5.8.5 If a Partner leaves the Agreement, decisions must be taken and followed through on what happens to:

- The information that has already been shared with the signatories by the departing organisation
- The information that has already been shared with the departing organisation by the other signatories

5.8.6 Where information is placed on Resilience Direct for information sharing purposes, the organisation that owns the information remains responsible for removing this information from Resilience Direct once it is no longer required.

5.9 ROLES AND RESPONSIBILITIES UNDER THIS AGREEMENT

5.9.1 All Partners to this Agreement must appoint Single Points of Contact (SPOC) along with a deputy to cover for sickness and holiday.

5.9.2 The appointed SPOC (and deputy) for each organisation can be found in Annex B.

5.9.3 The SPOC's or their deputy within each organisation will be the first port of call for questions about the Agreement. If there is a problem such as a potential information security breach, relevant SPOCs must be contacted.

5.9.4 It is the responsibility of everyone sharing, accessing and using the information to make appropriate decisions, then hold the information securely, in accordance with the standards set out in this Agreement (see Annex A). Any person who is not sure of the requirements on them should read this Agreement, then, if necessary, contact their SPOC.

5.9.5 Only appropriate and properly authorised persons will have access to the information specified in this Agreement. If in doubt, a person intending to share or access information should contact their SPOC.

5.9.6 Information shared between Partners must not be disclosed to any organisation outside the LRF without consulting the Partner that provided the information. For the purposes of this Agreement, a discussion regarding such sharing lies with the SPOC of the originating organisation.

5.10 REVIEW OF THE INFORMATION SHARING AGREEMENT

5.10.1 This Agreement will be reviewed six (6) months after its launch and every twelve (12) months thereafter by the LRF. Alterations are to be sent to LCC Emergency Planning and Business Continuity Service.

5.10.2 If a significant change takes place which means that the Agreement becomes an unreliable reference point, then the Agreement will be updated as needed and a new version circulated to replace the old.

5.10.3 If the SPOC or their deputy departs their role, an alternative lead must be nominated as soon as possible.

5.11 INDEMNITY

5.11.1 Recipient organisations will accept liability for a breach of this Information Sharing Agreement should legal proceedings be served in relation to any, failure, breach or default involving the received information. The recipient organisation cannot be held liable if a breach occurs that is attributable solely to any failure, breach or default on the part of the Information Provider.

6. SIGNATURES

6.1 By signing this Agreement, all signatories accept responsibility for its execution and agree to ensure that all staff are trained so that requests for information and the process of sharing are sufficient to meet the purpose of this Agreement.

6.2 Signatories must also ensure that they comply with all relevant legislation and with the provisions set out in the Minimum Information Security Standards set out at Annex A.

Signed on behalf of Anglian Water	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Animal and Plant Health Agency	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Boston Borough Council	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of British Red Cross (on behalf of the voluntary sector)	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of British Transport Police	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of BT	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of City of Lincoln Council	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of East Lindsey District Council	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of East Midlands Ambulance Service	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Environment Agency	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Highways England	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Lincolnshire Community Health Service	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Lincolnshire County Council	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Lincolnshire Fire and Rescue Service	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Lincolnshire’s Internal Drainage Boards	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Lincolnshire Partnership Foundation Trust	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Lincolnshire Police	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Maritime and Coastguard Agency	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Met Office	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of National Grid	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of NHS England – Central Midlands	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of NHS Lincolnshire East Clinical Commissioning Group	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of NHS Lincolnshire West Clinical Commissioning Group	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of NHS South Lincolnshire Clinical Commissioning Group	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of NHS South West Lincolnshire Clinical Commissioning Group	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Network Rail	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of North Kesteven District Council	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Northern Power Grid	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Public Health England	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Severn Trent Water	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of South Holland District Council	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of South Kesteven District Council	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of St Barnabas Hospice	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of United Lincolnshire Hospitals Trust	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of West Lindsey District Council	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

Signed on behalf of Western Power Distribution	
Print Name	
Position	
Date	
Print Name	
Position	
Date	

ANNEX A – MINIMUM SECURITY STANDARDS

1 General

1.1 Personal data shall be appropriately protected and only accessed for a lawful purpose at all times.

1.2 Personal data shall not be disclosed to any person or organisation unless authorised by LCC and as part of a written agreement e.g. information sharing agreement or written contract.

1.3 All staff involved in handling personal data shall complete locally arranged information security and data protection training.

1.4 A security policy must be in place which sets out management commitment to information security and data protection and defines information security and data protection responsibilities.

1.5 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 for the rights and freedoms of data subjects in relation to the processing of personal data. Any proposed transfers of personal data outside of the European Union must be approved in advance by the data controller.

2 Electronic Information

2.1 Electronic copies of personal data supplied shall only be stored:

2.2 On hardware located in premises which are secure. This means premises which have suitable security measures to prevent unauthorised access and to protect information and information assets. Security measures include control of access; locked windows and doors; intruder alarm; visitor control.

2.3 On portable devices e.g. laptops, netbooks, which are encrypted using AES-256 bit encryption.

2.4 On removable media e.g. USB memory sticks, CD's, DVD's and external hard drives which are encrypted using AES-256 bit encryption

2.5 Electronic personal data shall not be transferred to any system not under the control of the third party e.g. a private laptop belonging to a staff member.

2.6 The use of unencrypted portable devices or removable media to store personal data shall not be authorised.

2.7 Portable devices and removable media shall be held under lock and key when not in use; data stored on removable media for the purpose of transporting data shall be securely deleted immediately after use e.g. USB sticks, external hard drives.

2.8 Access control (username & password) shall be in place across any device which is used to store electronic personal data.

2.9 Passwords shall consist of a minimum of seven characters including a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols.

2.10 Electronic copies of personal data shall be securely deleted when no longer required (in line with retention and disposal schedules). This includes data stored on servers, desktops, laptops or other hardware and media. Secure deletion means deleting files so they cannot be retrieved.

3 Electronic Data Transfer

3.1 Data transfer shall occur in the following ways; by secure email; by secure file transfer; via a trusted private network (utilised for the exchange of information without data traversing the public internet); or by secure courier services.

3.2 Secure email – personal data sent by email shall be transferred by attachment to an email between nominated GCSX, NHS.Net, PNN, GSI, GSX email accounts. Staff shall use the email addresses notified to the other party in advance of the data transfer to ensure that the recipient confirms successful receipt before data is sent.

3.3 Where GCSX email transfer is unavailable then an alternative secure email service shall be used e.g. LCC Secure mail. A secure email service is one which uses an encrypted communication/connection to deliver the email. If in doubt about the intended use of a specific solution, advice is to be sought from LCC's Information Governance team before the transfer occurs.

3.4 Secure Courier – data transfer shall be achieved using a signature service provided by a reputable secure courier. Removable media used to store the data shall be encrypted using AES 256 encryption. Passwords must be communicated separately and are not to be included with the media.

3.5 The receiving party must confirm by email that they are ready for the transfer and that the recipient address is correct before the transfer takes place. A further email must be sent confirming when the recipient has received, intact, the data.

4 Network Security

4.1 Personal data stored on a device/network which connects to the public internet shall implement the following controls which offer a sound foundation of basic security:

4.2 Boundary firewall and internet gateways: Information, applications and computers within the organisation's internal networks should be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.

4.3 Secure configuration: Computers and network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

4.4 User access control: User accounts, particularly those with special access privileges (e.g. administrative accounts) should be assigned only to authorised individuals, managed effectively and provide the minimum level of access to applications, computers and networks.

4.5 Malware protection: Computers that are exposed to the internet should be protected against malware infection through the use of malware protection software. Examples of Malware include viruses, worms, trojan horses, ransomware, spyware, and adware.

4.6 Patch Management: Software running on computers and network devices should be kept up-to-date and have the latest security patches installed.

5 Hard Copy Information

5.1 Hard copy personal data which includes printed material, files, and documents shall be stored under lock and key when not in use and access to the information shall be controlled.

5.2 Anonymised information shall be used wherever possible.

5.3 When printing off personal data only print the minimum necessary to achieve your aim.

5.4 When transporting hard copy personal data a locked briefcase or bag shall be used and it shall remain in your custody at all times. The personal information must not be visible through the bag.

5.5 Personal data shall only be removed from premises when absolutely necessary and shall be returned and locked away as soon as possible.

5.6 Hard copy personal data shall be destroyed securely when no longer required e.g. cross cut shredder. Alternatively it can be returned securely to LCC for destruction if local facilities are not available.

5.7 Data transfer of hard copy personal data shall be achieved by signature service recorded delivery or courier service in a sealed envelope, addressed to an individual by name or appointment.

6 Security Incidents/Data Breaches

6.1 The third party must notify LCC immediately of any information which has been subject to an actual or potential security incident or data breach including any failure to comply with the security requirement set out in this schedule.

6.2 The third party must fully co-operate with any investigation that LCC requires as a result of a potential security incident or data breach.

6.3 In the event of a security incident or data breach data transfers shall be delayed until the risk or issue is resolved.

6.4 If a security incident or data breach cannot be resolved following intervention data transfers shall stop unless the risk of stopping the transfer of personal data is outweighed by the need to transfer the personal data. Authority to continue must be provided by the information owner.

ANNEX B – SINGLE POINT OF CONTACTS AND DEPUTIES
(Need to be identified)

Organisation	SPOC (name, address, telephone number, email)	Deputy SPOC (name, address, telephone number, email)