



Smarter studies  
Global impact  
Better health



## MANAGEMENT OF PERSONAL DATA

### VERSION 4.0

#### APPROVALS

Author and Position	Signature	Date
Stephen Townsend Clinical Project Manager for Data Science	DocuSigned by: <i>Steve Townsend</i> 72B77F4216C14ED...	27-May-2021
Reviewer(s) and Position	Signature	
Mary Rauchenberger Head of Data Management Systems	DocuSigned by: <i>Mary Rauchenberger</i> 5DEA25C1E04841E...	28-May-2021
Matthew Sydes Professor of Clinical Trials and Methodology	DocuSigned by: <i>Matthew Sydes</i> 2DB2A83FA918404...	27-May-2021
Joanna Calvert Trial Manager	DocuSigned by: <i>Joanna Calvert</i> 30F7C2B726294A7...	28-May-2021
Approver and Position	Signature	
Sheena McCormack Chair of Research Governance Committee	DocuSigned by: <i>Sheena McCormack</i> 5CD005D036AE49E...	14-Jun-2021

Name	Signature	Date uploaded to SOPbox
Steve Townsend	DocuSigned by: <i>Steve Townsend</i> 72B77F4216C14ED...	15-Jun-2021

The effective date of this SOP is the day on which it is uploaded to SOPbox and is available to us  
This is the date associated with the signature of the SOPbox Administrator.

For the Revision History please see the Version History Summary in SOPbox.

# MANAGEMENT OF PERSONAL DATA

## TABLE OF CONTENTS

<b>1</b>	<b>BACKGROUND AND RATIONALE.....</b>	<b>4</b>
1.1	UNDERSTANDING WHAT IS MEANT BY PERSONAL DATA .....	4
<b>2</b>	<b>PURPOSE.....</b>	<b>6</b>
<b>3</b>	<b>RESPONSIBILITY AND ROLES .....</b>	<b>7</b>
<b>4</b>	<b>PROCEDURES.....</b>	<b>9</b>
<b>4.1</b>	<b>GENERAL PRINCIPLES OF MANAGING STUDY PARTICIPANT PERSONAL DATA.....</b>	<b>9</b>
4.1.1	Directly Identifiable Data .....	10
4.1.2	Managing Directly Identifiable Data .....	11
4.1.3	Storage of Directly Identifiable Data .....	11
4.1.4	Sending and Receiving Directly Identifiable Data .....	11
4.1.5	Requesting Access to Directly Identifiable Data .....	13
4.1.6	Indirectly Identifiable Data .....	13
4.1.7	Managing Indirectly Identifiable Data .....	14
4.1.8	Storage of Indirectly Identifiable Data.....	14
4.1.9	Sending and Receiving Indirectly Identifiable Data .....	14
4.1.10	Externally Provided Databases .....	15
<b>4.2</b>	<b>DATA PROTECTION IMPACT ASSESSMENT (DPIA) .....</b>	<b>15</b>
4.2.1	When is a DPIA required?.....	16
4.2.2	When to complete a DPIA .....	16
4.2.3	What must be contained .....	16
<b>4.3</b>	<b>DATA REQUESTS FROM PARTICIPANTS .....</b>	<b>17</b>
<b>4.4</b>	<b>MANAGING NON-STUDY PERSONAL DATA.....</b>	<b>17</b>
<b>4.5</b>	<b>REPORTING PERSONAL DATA BREACHES.....</b>	<b>18</b>
<b>5</b>	<b>RELATED DOCUMENTS.....</b>	<b>19</b>
<b>6</b>	<b>APPENDIX 1.....</b>	<b>20</b>
6.1.1	Getting Started .....	20
6.1.2	Receiving emails with Galaxkey – Using the Website.....	25
6.1.3	Using Galaxkey to transfer large file – Galaxkey Workspace (supersedes Galaxkey Secure Share (GSS)) .....	26
6.1.4	Galaxkey Workspace – For External Users .....	29
<b>6.2</b>	<b>7-ZIP.....</b>	<b>29</b>

**Note:** Glossary of terms, acronyms and abbreviations will be provided in a separate document for all SOPs and associated documents

The following symbols may be used in this SOP:



Indicates a link to a related document



Indicates instructions to document study-specific processes elsewhere

Throughout this document 'MRC CTU' will be used to refer to the MRC Clinical Trials Unit at UCL (MRC CTU at UCL).

## 1 BACKGROUND AND RATIONALE



The personal data which is collected during the running of studies at MRC CTU is processed in order to answer the study questions. The ways in which the data is processed is guided by:



1. The EU General Data Protection Regulation (GDPR) – harmonisation of data privacy laws across Europe, which came into effect from 2018.
2. UK Data Protection Act 2018 – this is the UK’s implementation of the General Data Protection Regulation (GDPR) into British law.



It is also impacted by the Clinical Trials Directive and Good Clinical Practice but this SOP will deal mostly with how we collect and manage personal data in line with GDPR and the UK Data Protection Act.



When working with international collaborators (especially those outside the European Economic Area (EEA)), it is important to consider any differences in international law regarding the management of personal data.









### 1.1 UNDERSTANDING WHAT IS MEANT BY PERSONAL DATA

	<b>What is personal data?</b>
	The GDPR defines personal data as ‘ <b>any information relating to an identified or identifiable living individual</b> ’ who can be <b>identified either directly or indirectly</b>

	<b>Can we treat the data from study participants who have passed away differently?</b>
	No, personal data of those who have passed away is covered by the <b>Common Law Duty of Confidentiality</b> , which means we still have an ethical and legal obligation to protect their data as we would if they were living.

	<b>There aren't any identifiers in my dataset like name, address, or date of birth. I only have study number, so is it still personal data?</b>
	Yes, it probably is. Does it contain other data, which in combination could be identifiable, e.g. site name, date of visit, times of tests, descriptions of events, etc., could someone potentially identify them from this? This is called <b>pseudonymised data, which is still personal data</b> and must be managed as such. In fact, the data we collect and process is actually considered to be a <b>special category of personal data</b> .

	<b>What is a special category of personal data?</b>
	It is any particularly sensitive personal data, relating to, amongst other things, <b>health, sex life or sexual orientation, racial or ethnic origin and genetic or biometric data</b> .

	<b>Do special categories of personal data need to be handled differently to other personal data?</b>
	Yes, to be able to process data of this nature we need to implement <b>appropriate safeguards</b> to protect the data and ultimately protect the rights and safety of the participants. A Data Protection Impact Assessment (DPIA) must be completed for studies using special category data. The DPIA template can be downloaded from the Data Protection section of the UCL website.
	<b>What sort of safeguards should we be using?</b>
	The phrase used in GDPR is ' <b>Data protection by design and by default</b> '. Which means we must always be conscious of how we are managing personal data. Some of the types of safeguards we can use are <b>pseudonymisation, minimisation and encryption</b> .
	<b>What is minimisation in relation to GDPR?</b>
	It means <b>only collecting the data you need and plan to use in line with the study protocol</b> .
	<b>Is anonymised data still considered personal data?</b>
	No, truly anonymised data, i.e. data from which it is <b>impossible</b> to identify individuals, e.g. aggregate data, is not considered personal data.

## 2 PURPOSE

The purpose of this SOP is:

- To define what constitutes personal data
- To outline the principles for the management of personal data, to ensure that confidentiality is maintained
- To define the MRC CTU roles and responsibilities involved in collecting, handling, communicating and storing personal data, with particular focus on personal data relating to study participants

### 3 RESPONSIBILITY AND ROLES

The following table lists the roles relevant to this SOP and a brief description of their responsibilities.

This SOP will be circulated for Read and Understood to all appropriate roles identified in the training matrix.

ROLE	RESPONSIBILITIES
All Staff including those holding Honorary contracts, visiting workers and students	<ul style="list-style-type: none"> <li>• Anyone who comes into contact with personal data must abide by the principles of this SOP</li> </ul>
Trial/Study Management Team (TMT) including a Data Management Systems and Statistics representative	<ul style="list-style-type: none"> <li>• Ensure only essential personal data is collected for the purposes of the study</li> <li>• Where the essential personal data required exceeds the stated minimums in this SOP, this must be outlined in the risk assessment</li> <li>• Ensure the study database does not hold any directly identifiable data (see section 4.1 for definitions)</li> <li>• Ensure that any personal data which is transferred outside of the unit is done securely</li> <li>• Ensure appropriate approval is in place from the Research Governance Committee (RGC) for the use of any directly identifiable data in any analyses</li> <li>• Register new studies with the UCL Data Protection Office</li> <li>• Complete the Data Protection Impact Assessment</li> <li>• Ensure RGC is informed of any potential data breaches</li> </ul>
Data Management Systems	<ul style="list-style-type: none"> <li>• Provide expertise and advice on best practice for the collection and storage of personal data</li> <li>• Ensure appropriate databases are in place to hold any information required for a study</li> </ul>
IS Servicedesk	<ul style="list-style-type: none"> <li>• Provide advice and guidance on best practice for the sending and receiving of personal data electronically</li> <li>• Assist in registering new studies with the Data Protection office at UCL as needed</li> <li>• Assist in reporting Breach of Personal Data forms and liaising with the UCL Data Protection Office</li> </ul>
Statistics functional group	<ul style="list-style-type: none"> <li>• Ensure analysis files hold minimal indirectly identifiable data</li> </ul>
Meta-Analysis functional group	<ul style="list-style-type: none"> <li>• Ensure appropriate approval is in place from the Research Governance Committee (RGC) for the use of any directly identifiable data in any analyses</li> <li>• Ensure analysis files hold minimal indirectly identifiable data</li> </ul>

Research Governance Committee (RGC)	<ul style="list-style-type: none"><li>• Review and approve proposed collection and handling of personal data in line with the principles of this SOP</li><li>• Assess, and approve if agreed, any access to directly identifiable data.</li><li>• Review, and approve if needed, any data access or amendment requests made by participants through the UCL Data Protection Officer.</li><li>• Review and assess impact and any required actions for breaches of personal data.</li><li>• Review and approve a study using more than the recommended number of indirect identifiers</li></ul>
Contracts	<ul style="list-style-type: none"><li>• Ensure the appropriate safeguards around data security are included in data sharing agreements</li></ul>



## 4 PROCEDURES

In general, all data collected for the purpose of MRC CTU at UCL studies are personal data. Therefore, study data must always be treated in accordance with the principles of this SOP.

New studies must be registered with the Data Protection Office in UCL. Contact the IS service desk for assistance in completing the registration form.



See the UCL website for more information and registration form <https://www.ucl.ac.uk/data-protection>



See the Sponsorship of MRC CTU at UCL Studies SOP

### 4.1 GENERAL PRINCIPLES OF MANAGING STUDY PARTICIPANT PERSONAL DATA

These principles apply to anyone based within the MRC CTU who may come into contact with participant personal data.

1. All staff who will handle personal data in the course of their jobs must complete the appropriate training courses, including refresher courses, in line with current unit guidance:
  - a) Information Security
  - b) GDPR Training
  - c) This SOP, Management of Personal Data
2. Only essential personal data should be collected. Conditions of funders on the sharing of research data must also be considered when defining essential personal data required.
3. Participant personal data should be pseudonymised with the use of a study number. Participants must not be identifiable to the study team, i.e. those people processing the data must not have access to the direct identifiers.
  - a) The exception to this principle is collection of directly identifiable information over the phone during a randomisation call. This is the only time directly identifiable data are available to study teams. There is no continued access to these data for the study teams.
4. Only those with appropriate authorisation, as documented on a study delegation log and/or as recorded in STOPover, should be able to access study participant personal data. For example, data collected as part of a study must only be accessible to the study team. There may be instances where individuals outside of the study team require access to the data, but permission for this must have been sought first from the RGC.
5. Where participant personal data is accessed via database systems, individuals with access to those systems must never share their passwords with other people. This also applies to site staff entering personal data remotely. Site staff entering data are expected to sign a Non-Disclosure of Password Agreement



See the non-disclosure of password agreement template available in SOPbox

6. Where participant personal data is being transferred electronically e.g. via email, it is expected to be encrypted, using strong methods of encryption such as Galaxkey.
7. Sites should be given guidance on how we would prefer to receive participant personal data and should be encouraged to follow that guidance. In some instances, sites and/or collaborators may have their own preferred secure data exchange mechanisms. In such cases, study teams are advised to seek advice from the MRC CTU Information Servicedesk (IS) and Data Management Systems (DMS) departments with respect to the appropriateness of such a system. Advice and methods for how we prefer to receive data must also be documented in the Data Management Plan (DMP).
8. All staff members must ensure that their computer screen is locked when moving away from their desk. Any personal data on paper must also be locked away when not in use.
9. Once all CTU activities have been completed and the study has ended, personal data will be archived in accordance with unit procedures.



See the Long Term Storage Procedures for Paper Documents & Database Archive SOPs

10. Where there is a breach of data protection or a near miss this must initially be reported by contacting RGC (using the RGC notification form) and copying in the IS Servicedesk. The RGC must be kept informed at all stages and any onward reporting must be discussed with RGC prior to any action being taken. The IS Servicedesk will assist in completing the Personal Data Breach Reporting Form as appropriate, and sending to the UCL Information Security Group email address ([isg@ucl.ac.uk](mailto:isg@ucl.ac.uk)) as soon as possible if RGC decide this is necessary. Depending on the nature of the issue and who the Data Controller is, the breach will be escalated onward as appropriate.



See the Personal Data Breach Reporting Form on the UCL website to use when reporting a personal data breach

#### 4.1.1 DIRECTLY IDENTIFIABLE DATA

Definition - Any data item that requires minimal effort by an educated third party to identify an individual.

Typical direct identifiers would include:

- Name
- NHS number
- CHI Number
- Photographs containing identifying features e.g. facial photographs
- Full postcode
- Postal address
- Contact details such as telephone numbers or email addresses.
- Internal hospital number

Such data requires special handling, and must be kept separately from the main trial database(s) with no access to the data by the trial team. The recommended method for doing so is to use the UCL Data Safe Haven (DSH), which is only accessible by DMS administrators on request by the trial team and with permission from RGC. If re-identification will be required in the future, e.g. for linkage purposes, they can be stored with a code such as study number.

#### 4.1.2 MANAGING DIRECTLY IDENTIFIABLE DATA

Any collection of directly identifiable data, and the intended processes for handling these data appropriately, must be discussed with Data Management Systems and then be reviewed and approved by the RGC.



Detail the directly identifiable data planned for collection and the intended methods of handling that data in your study Risk Assessment

#### 4.1.3 STORAGE OF DIRECTLY IDENTIFIABLE DATA

If a study has a requirement to collect directly identifiable data, this must be approved by RGC and the participant must give consent to store these data. The data must be stored separately from the main trial database and any other identifiable data, ideally storing these data in the DSH. Access to directly identifiable data will generally be restricted to key personnel within the Data Management Systems Group, and be limited to RGC approved reasons for access, such as a survival sweep with the Office for National Statistics (ONS).

In the unusual instance where the trial team require access to directly identifiable data, this must also be approved by the RGC, and will ideally take place within the Data Safe Haven. This also applies to any planned analyses that will use identifiable data.

If there are any unplanned analyses which arise during the course of a study, which require the inclusion of identifiable data, the trial team must seek additional permission to use these data from the RGC. Following analyses using directly identifiable data, copies of the raw data must be securely destroyed.

#### 4.1.4 SENDING AND RECEIVING DIRECTLY IDENTIFIABLE DATA

##### 4.1.4.A Electronically

Sending of data with directly identifiable data items (e.g. name, NHS number) must only be performed by the responsible individuals in the Data Management Systems team. If this is for the purposes of obtaining “flagging information”, for example from national registries, the procedures agreed with the relevant registry must be followed as well as the internal procedure i.e. encrypted and password protected.

Any directly identifiable data received unexpectedly in an email, such as name, must be removed from any subsequent email response. This email must then be deleted from the email inbox and deleted items folders. If this happens, remind collaborators not to send directly identifiable data electronically.

If there is a trial design where collection and storage of directly identifiable data is required, then these must be approved by RGC. Careful consideration must be given to processes to ensure minimal data collection and secure processing. This may include using the UCL Data Safe Haven

(DSH) for storage and deleting any other form of communication within the day of receipt (such as forms received via Galaxkey).

#### 4.1.4.B Receipt of Electronic Communications from Participants

Direct communication with trial teams from participants, is not invited but may still happen. In the unlikely event that a study team receives communication directly from a participant or their family, e.g. via email, the communication must be sent via a secure method (such as secure email) to a single member of the study team to deal with to ensure control is kept on the whole of the process and to minimise the number of people who are aware of the participant's identity. Ideally, the response would come from the trial clinician, using an nhs.net email account if possible.

The following points must be considered and clearly communicated to the participant:

- The trial team cannot provide direct medical advice. This must be sought from the local care team
- All emails, other than those retained in an nhs.net email account for clinical purposes, will be deleted to ensure protection of their personal data
- Where to find further information and resources, if applicable

The original email must be removed from the inbox of whomever received the original email following a response, and any related folders such as the sent or deleted items. The nominated individual must also delete the email trail once correspondence has finished, from their email inbox folders (other than those retained in an nhs.net email account for clinical purposes). For any information that is being stored, consideration must be given to making sure that the information cannot be used to link the communicating participant to being part of a clinical trial, or to a specific participant in a trial.

#### 4.1.4.C Paper

Directly identifiable data received in paper format should generally not be kept at the CTU and trial working practices must be designed in such a way that this is not expected. Data of this nature must only be held electronically where permission has been granted for its collection. The RGC must approve any collection of directly identifiable data (via the Risk Assessment), and be consulted for any issues relating to storage of directly identifiable data.

If any directly identifiable data is planned and approved by RGC for initial collection on paper, e.g. Consent forms, then the TMT must ensure that this paper copy is destroyed via the confidential waste system once the data has been entered onto the appropriate database. It is expected that these approved documents containing directly identifiable data will be processed within 1 working day, and will be kept for no longer than 1 working day and must be stored in a secure area such as a lockable cupboard prior to processing.

Ideally, CRFs must not be used to collect directly identifiable data. If this is necessary then the CRFs must be designed such that this particular data is reported on a section of the form that can be removed and destroyed, leaving any other data to be stored securely with the trial CRFs. These must be double wrapped for extra security and sent to the MRC CTU using a tracked or signed for system to prevent potential loss of data in transit. There is also the option of a PO Box Collect service, depending on the nature of the data being collected in this way.

If a site mistakenly sends directly identifiable information, for example a participant's name which has been written on a CRF or supporting documentation, it must be obscured from the page, e.g.

with a black marker, and then the page photocopied to ensure the information is not still visible. The original page must then be confidentially destroyed. The study team should also remind the sender to remove direct identifiers before sending.

Directly identifiable data recorded on paper documents must never be taken out of the office.

#### 4.1.4.D Phone

Where sites telephone the CTU to randomise patients, full name or NHS number can be given, providing the rationale and process for handling and storing this data has been outlined in the risk assessment and the appropriate participant consent has been obtained. These data are collected over the phone by the internal randomisers group, made up of Trial Managers, Data Managers and Trial Assistants from trials across the Unit who have been trained appropriately



See the Training Policy for details of training requirements for new staff members

Such direct identifiers must be saved separately from the trial randomisation data, as described in section 4.1.3.

At no other time should a patient name be used in any contact with sites.

#### 4.1.5 REQUESTING ACCESS TO DIRECTLY IDENTIFIABLE DATA

When the TMT requires access to the directly identifiable data for the pre-approved purpose (See Section 4.1.1-3), they should submit a request to Data Management Systems. The data will only be released to an approved user, usually the trial statistician, ideally within the Data Safe Haven.

#### 4.1.6 INDIRECTLY IDENTIFIABLE DATA

Definition - Any data item that is unlikely to identify a person when looked at alone, but in combination could lead to identification and therefore become personal data.

Typical indirect identifiers would include:

- Date of Birth
- Participant Initials
- Soundex
- Age
- Gender
- Height
- Weight

Any of these data items alone would not allow you to identify someone. However, if some of these were put together, with the right context, an educated third party could identify that person without too much effort. Therefore, any combination of data that we hold for a study is likely to constitute indirectly identifiable personal data and must therefore always just be treated as such.

#### 4.1.7 MANAGING INDIRECTLY IDENTIFIABLE DATA

When a participant is recruited into a study a maximum of two indirect participant identifiers in combination with the allocated study number should be sufficient to identify the participant in the future e.g. to ensure a CRF is for the correct participant. Maintaining the accuracy of personal data is a principle of the GDPR, therefore this is an important factor for ongoing data collection and entry. If more than the recommended two indirect are being used then this must be recorded in the Risk Assessment documentation and approved by RGC.

Decisions regarding the use of these identifiers may be dependent on:

- Study specific factors e.g. strength of the trial numbers used or nature of the data,
- Country specific rules regarding the collection of specific identifiers e.g. full date of birth may not be available in all European countries depending on interpretation of GDPR.



If a study requires more than the recommended number of indirect identifiers to be collected this must be detailed in the Risk Assessment and approved by the RGC.

#### 4.1.8 STORAGE OF INDIRECTLY IDENTIFIABLE DATA

Indirectly identifiable data may be stored in the main study database. The standard security model would be applied to this data, such as controlled database access via delegation logs.

Appropriate access restrictions must also be applied to data of this nature which is held external to the study database. A few ways to achieve this are to ensure folders on the network containing this data are restricted to trial team members only and always locking your computer when you are away from your desk.

Documents, including CRFs, which hold indirectly identifiable data must always be stored in a locked drawer or cabinet. Documents of this nature must not be left out in the open when not in use.

When it is necessary to take data out of the office, electronic data must be held on an encrypted device, and paper documents must be packaged securely. The documents are expected to be in a double sealed envelope, with the inner envelope self-addressed with instructions to post to the MRC CTU.

Where possible, statistical analysis files will only hold minimal indirectly identifiable data, needed for the analyses. It will also be stored in a secure location only accessible to the person/s performing the analysis

#### 4.1.9 SENDING AND RECEIVING INDIRECTLY IDENTIFIABLE DATA

##### 4.1.9.A By post

For trials where CRFs are still being sent via post, the following CRFs must be sent by a more secure method than standard 1<sup>st</sup> or 2<sup>nd</sup> class post. This is not the preferred method for collecting CRFs

containing these data, see Section 4.1.9.B for using electronic methods of sending and receiving data.

- CRFs collecting particularly sensitive data, which would lead to direct identification of participants e.g. for very rare conditions.
- CRFs with contact details (e.g. Name, full postcode, email addresses etc.)

All other CRFs or data queries can be sent in a sealed envelope by ordinary post.

#### **4.1.9.B Electronically or by fax/eFax**

The Study Number should be the only identifier used in any email/efax communication with sites or collaborators. If Study Number plus any other indirect identifier is being used, the file must be sent securely. The current unit approved method of encryption is Galaxkey.

It is important to consider the content of the communication and who is receiving it, and limit the amount of information that describes details about the participant, particularly outside the clinic team who looks after them. If more detail is required, then the communication should be sent securely.

See Appendix 1 for further instructions on using Galaxkey and what to do if an alternative method is required.

Collaborators should be encouraged to use secure methods when sending data electronically if it contains indirect identifiers. Any data received electronically which has not been protected must be handled appropriately in line with the principles of this SOP. Further electronic communication of this data is expected to be sent securely as per the instructions in Appendix 1, or the file can be removed to a secure area on the network.

#### **4.1.10 EXTERNALLY PROVIDED DATABASES**

Where UCL is the sponsor or where MRC has been delegated responsibility for database development and maintenance, if a trial or study uses a database which has been developed by a provider external to the MRC CTU, this must have been discussed, and approved by the RGC. Part of this process must be an exploration of the suitability of the database with regard to security, which may involve consultation with the Information Governance team at UCL, including how far it meets the principles detailed in this SOP.

Where UCL is not the sponsor or where MRC has not been delegated responsibility for database development, the sponsor's processes may be followed when assessing the suitability of externally provided database systems.

## **4.2 DATA PROTECTION IMPACT ASSESSMENT (DPIA)**

A DPIA is a way for you to systematically and comprehensively analyse your processing and help you identify and minimise data protection risks separately, but in addition to, the Trial Risk Assessment documentation (Risk Assessment/Risk Register). DPIAs must consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material or non-material. It is a key part of the new focus on accountability and data protection by design.

To assess the potential for disadvantage, a DPIA must consider both the likelihood and the severity of any impact on individuals. A DPIA does not have to indicate that all risks have been eradicated, but it will help you document them and assess whether or not any remaining risks are justified.

#### 4.2.1 WHEN IS A DPIA REQUIRED?

A DPIA must be completed for any type of processing that is likely to be high risk. This includes processing special category data, which includes data concerning health.



See the UCL website for more information on special category data <https://www.ucl.ac.uk/data-protection>

It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

#### 4.2.2 WHEN TO COMPLETE A DPIA

You must do a DPIA before you begin any type of processing that is likely to carry a high risk because of the nature of the data.

#### 4.2.3 WHAT MUST BE CONTAINED

A DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. The potential for negative impact or significant disadvantage results from a data breach that causes some harm happening frequently or to a larger proportion of participants, or a data breach that causes serious harm affecting a small proportion of participants, even if it's a rare event.

You may consult the MRC CTU IS Service Manager (via the Servicedesk) and, where appropriate, individuals and relevant experts. The MRC CTU IS Service manager will inform the data protection officer as required. Any processors may also need to assist you.



Contact the Servicedesk at: [mrcctu.isservicedesk@ucl.ac.uk](mailto:mrcctu.isservicedesk@ucl.ac.uk)

If a high risk that cannot be mitigated is identified, the risk must be discussed with the RGC, and the Information Commissioner's Office (ICO) must be consulted before starting the processing of the data.

The IS Service Manager will liaise with the UCL Data Protection Office as appropriate to ensure contact with ICO is made appropriately.

- The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, the ICO may issue a formal warning not to process the data, or ban the processing altogether.





See the ICO website for more information: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>



A template is available from the UCL website, under data protection for you to use to complete a DPIA: <https://www.ucl.ac.uk/data-protection/>

### 4.3 DATA REQUESTS FROM PARTICIPANTS

As part of the principles of GDPR participants are able to make requests in regards to the data the Unit holds about them e.g. to access personal data held by MRC CTU at UCL about themselves. These requests must go through the UCL Data Protection Officer (at [data-protection@ucl.ac.uk](mailto:data-protection@ucl.ac.uk)) as described in the UCL and MRC CTU at UCL privacy notices, available on the respective websites.



See the UCL website for the UCL privacy notice : <https://www.ucl.ac.uk/legal-services/privacy/>



See the MRC CTU at UCL website for the MRC CTU at UCL privacy notice : <https://www.ctu.mrc.ac.uk/privacy/>

All requests must be discussed by the TMT and RGC, with approval from RGC required depending on the risk to existing study data. Participants withdrawing their consent must be managed according to the Managing Early Cessation of Study Participation SOP.



See the Managing Early Cessation of Study Participation SOP

### 4.4 MANAGING NON-STUDY PERSONAL DATA

In the course of our work we collect and process personal data from other sources than study participants. For example during recruitment, or as part of the Patient and Public Involvement work which is done in the unit. In all instances, the principles below must be adhered to:

1. Only essential personal data may be collected.
2. Where appropriate those for whom we hold and process personal data must be made aware of this
3. Only those with appropriate authorisation are able to access personal data.
4. Where participant personal data is accessed via database systems, individuals with access to those systems must never share their passwords with other people.
5. Where personal data is being transferred electronically e.g. via email it must be encrypted, using strong methods of encryption such as Galaxkey.
6. All staff members must ensure that their computer screen is locked when moving away from their desk. Any personal data on paper must also be locked away when not in use.
7. Where there is a breach of data protection or a near miss this must initially be reported by contacting RGC (using the RGC notification form) and copying in the IS Servicedesk. The RGC must be kept informed at all stages and any onward reporting must be discussed with RGC prior to any action being taken. The IS Servicedesk will assist in completing the Personal Data Breach Reporting Form as appropriate, and sending to the UCL Information Security Group

email address ([isg@ucl.ac.uk](mailto:isg@ucl.ac.uk)) as soon as possible if RGC decide this is necessary. Depending on the nature of the issue and who the Data Controller is, the breach will be escalated onward as appropriate.



Complete the Personal Data Breach Reporting Form on the UCL website to report a personal data breach

#### 4.5 REPORTING PERSONAL DATA BREACHES

A personal data breach is defined as resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Some examples of breaches would be:

- Study database accessed by an unauthorised individual
- Sharing of database login and passwords
- Malicious alteration or deletion of personal data
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen

If there is a breach of data protection, or a near miss, the initial response will be led by the MRC CTU IS Service Manager, who will co-ordinate the relevant activities and the completion of the Personal Data Breach Reporting Form. This form shall be sent to the UCL Information Security Group email address ([isg@ucl.ac.uk](mailto:isg@ucl.ac.uk)) as soon as possible. RGC will be informed and kept updated at all stages of the process. Depending on the nature of the issue and who the Data Controller is, the breach will be escalated onward as appropriate. This must be discussed with RGC prior to any further action being taken.

## 5 RELATED DOCUMENTS

For further information on this topic, see also:

- Informed Consent Development SOP
- Data Sharing SOP
- Risk Assessment SOP
- Long-term Storage of Paper Documents SOP
- Information Commissioner's Office website: <https://ico.org.uk/>

## 6 APPENDIX 1

### 6.1 GALAXKEY

Galaxkey is the preferred product for sending and receiving participant personal data at the MRC CTU at UCL. For MRC CTU staff to use Galaxkey an individual licence is required, licences are controlled by the unit Information Services (IS) department who can be contacted to grant access to and install the product. Collaborators who are receiving data or sending data to the MRC CTU via Galaxkey do not require a licence, rather they are invited to connect to the system via a licenced user at the MRC CTU.

Galaxkey enables secure data transfer by email or file transfer (recommended for larger files) via use of encryption keys linked to email address usernames and passwords. The system secures emails and data is transferred such that the user with the recipient address can use their email address to decrypt the email.

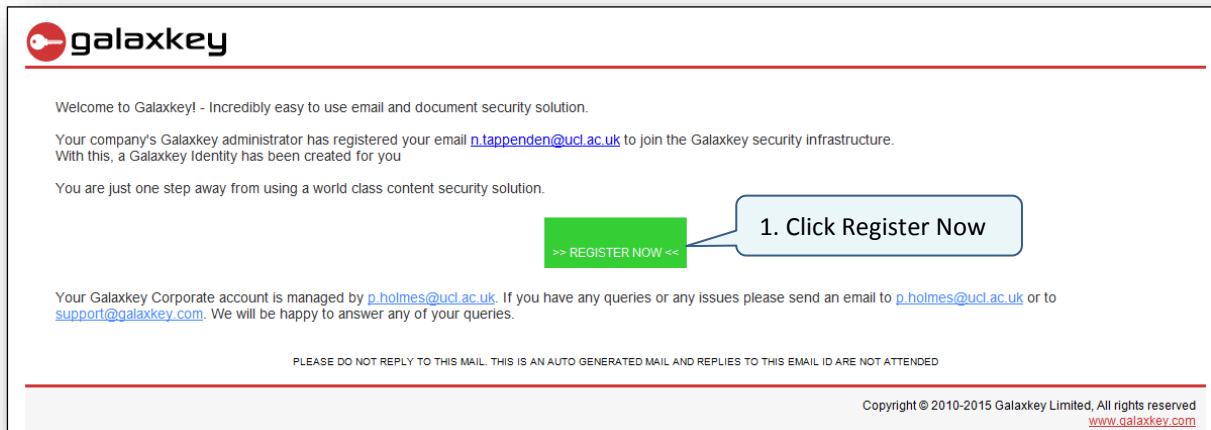
Galaxkey can be used as a plug-in embedded within Outlook, alternatively a web-browser based version is available.

The following steps describe how to use Galaxkey

#### 6.1.1 GETTING STARTED

Once you have been granted a licence to the system from IS, you will receive an email invitation to register as shown below.

Follow the steps in the screenshots as shown:



The registration form is titled "I am new to Galaxkey" in a red header. It contains the following fields and elements:

- Login ID \***: A dropdown menu.
- Name \***: A text input field.
- Password \***: A text input field.
- Confirm Password \***: A text input field.
- I accept the [Terms and Conditions](#) for registering a new account.
- REGISTER**: A red button.

Callouts on the right side of the form:

- 2. Click I am new to Galaxkey
- 3. Enter your name and create a password
- 4. Click to accept the Terms and Conditions and then click Register

5. The following screen opens and you can download the software from here if you have permissions to do so (if you do not have the relevant permissions, IS will need to download and install the software)

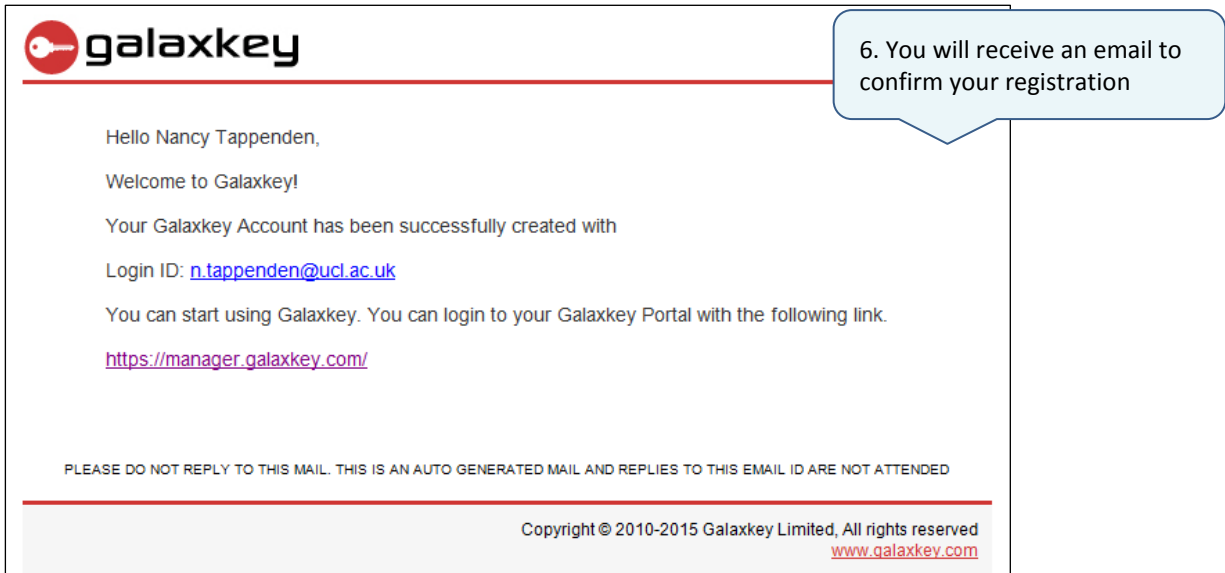
**Registration & Identity Acceptance**

Congratulations, we have created a new Galaxkey Account for you with Login ID **nancytappenden@hotmail.com**.

The identity with email address **nancytappenden@hotmail.com** has been added to this account

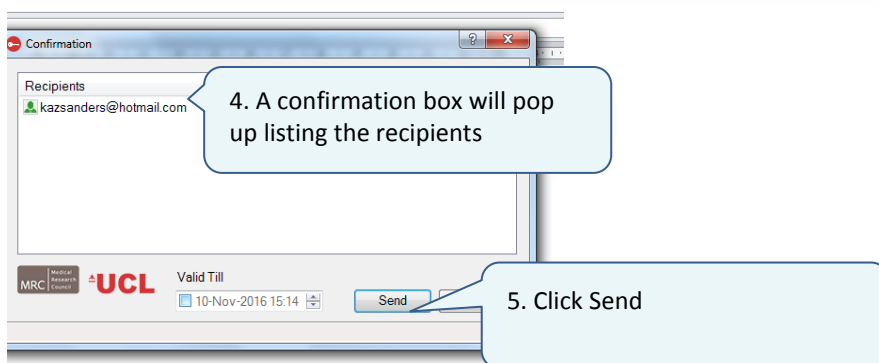
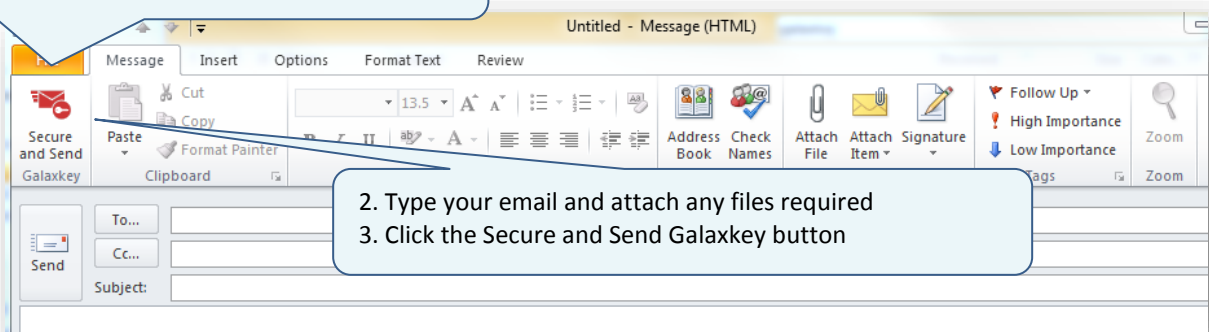
Please download the Galaxkey Client from the following links

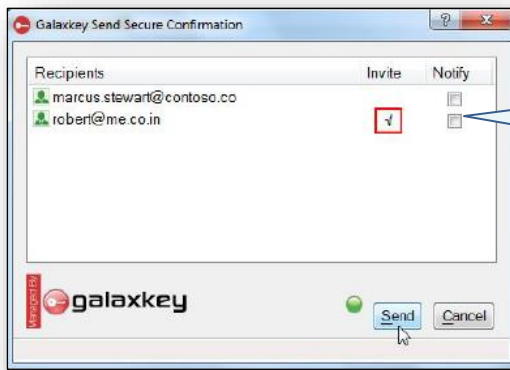
Download for Windows | ANDROID APP ON Google play | Download on the App Store | BlackBerry World | Download for Mac OSX



### 6.1.1.A Sending emails with Galaxkey – Using Outlook

1. When you open a new email the Secure and Send button will be visible





7. If you have not emailed a recipient using Galaxkey before it will generate an invite to them

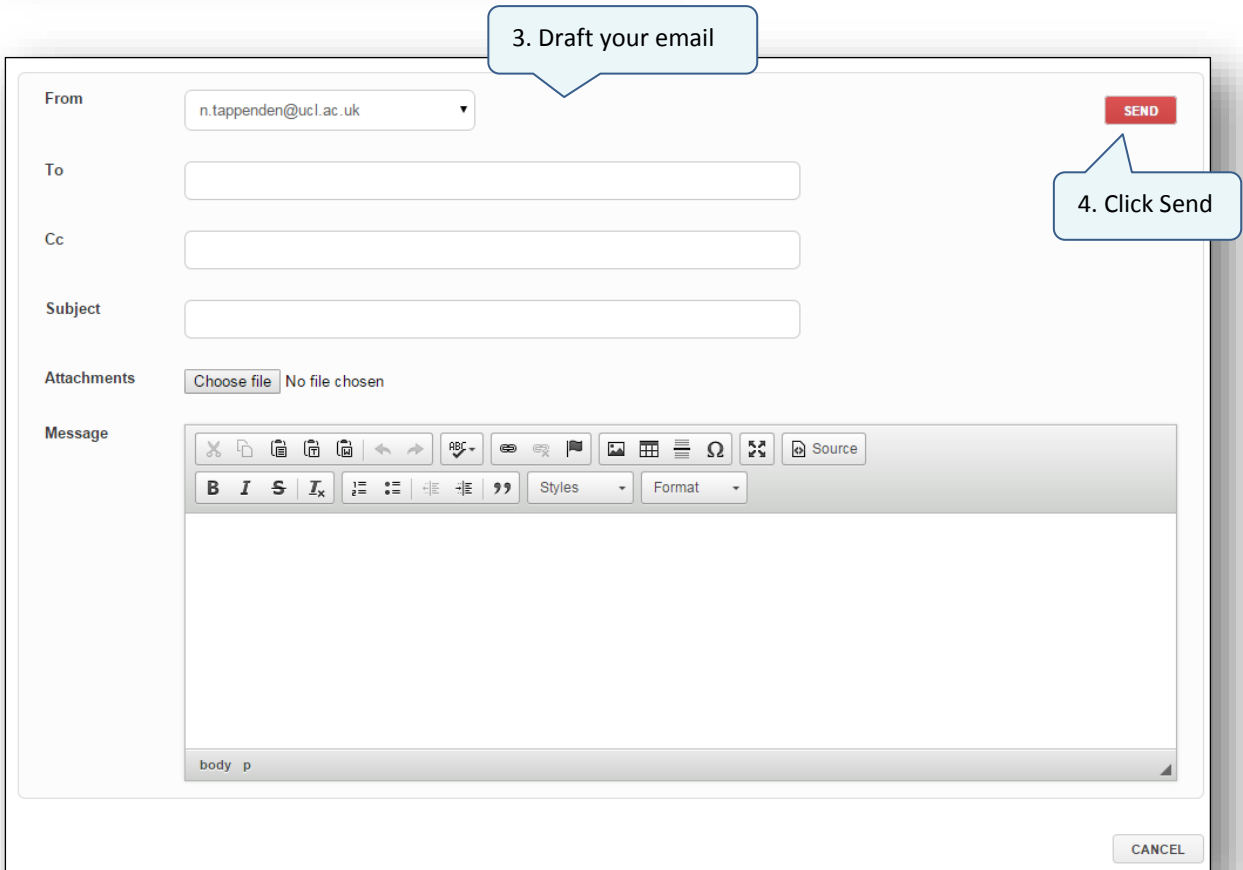
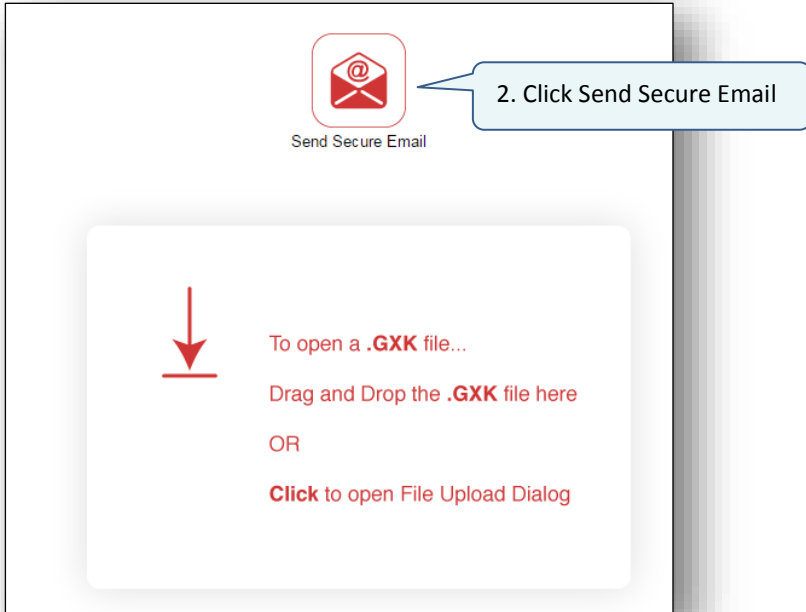
The email and any attachment will then be sent securely to the recipients.6.1.2b. Sending emails with Galaxkey – Using the Website

The Galaxkey website <https://gwa.galaxkey.com> can be used as an alternative to using the Outlook plug in.

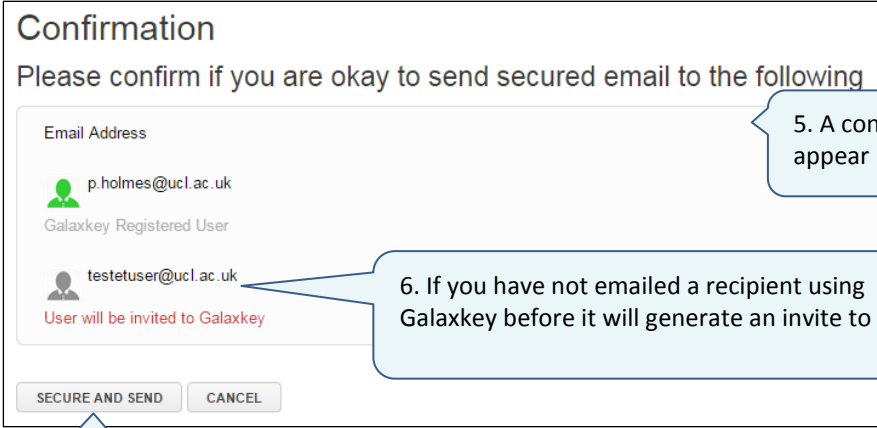
You can use the website to send secure email if:

- you were unable to download the software
- you are using a device on which the software has not been downloaded

1. You will be prompted to login









**Confirmation**

Please confirm if you are okay to send secured email to the following

Email Address

 p.holmes@ucl.ac.uk  
Galaxkey Registered User

 testetuser@ucl.ac.uk  
User will be invited to Galaxkey

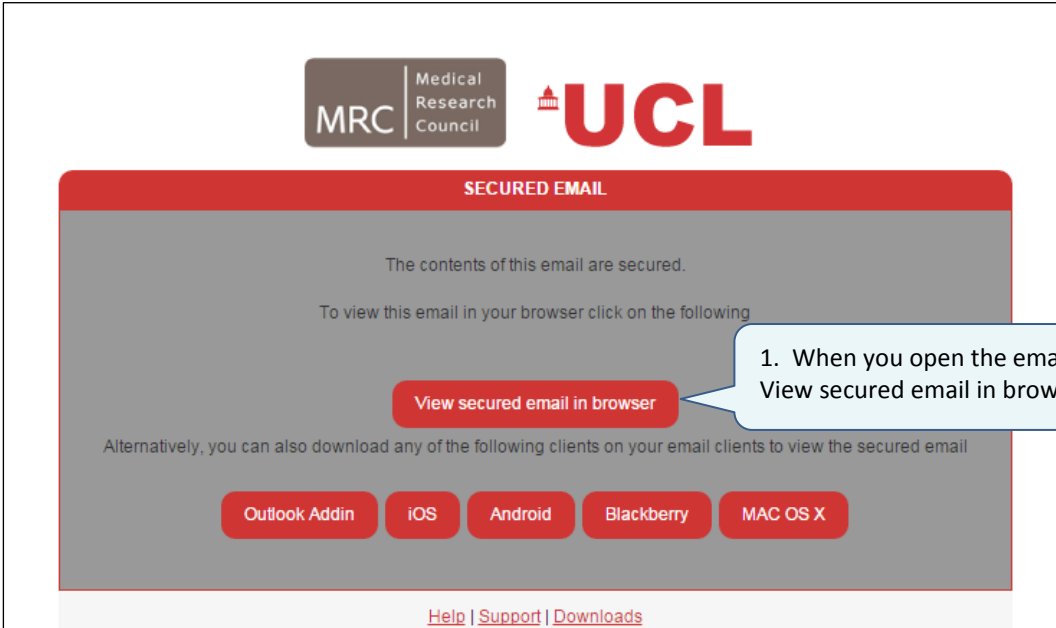
5. A confirmation screen will appear

6. If you have not emailed a recipient using Galaxkey before it will generate an invite to them

7. Click Secure and Send

### 6.1.2 RECEIVING EMAILS WITH GALAXKEY – USING THE WEBSITE

When sending information to collaborators using Galaxkey, if they have installed the plug-in following their initial invitation to Galaxkey (see step 1) then they will be able to view the email and attachments within Outlook. If the collaborator is unable to install the plug-in, they can access the email via the web-browser as follows:



MRC | Medical Research Council | UCL

**SECURED EMAIL**

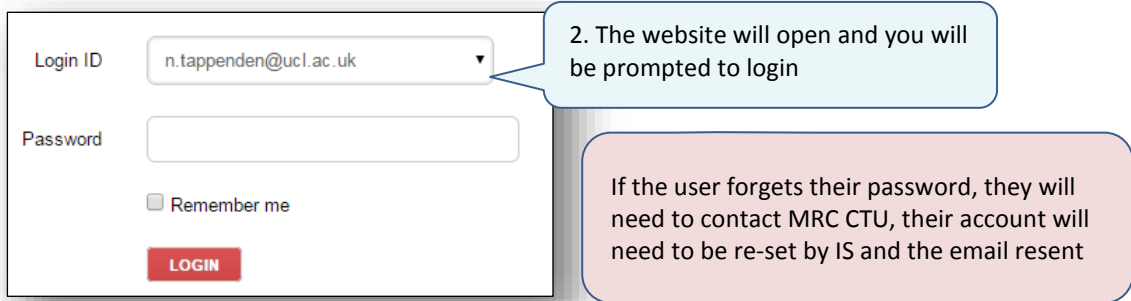
The contents of this email are secured.

To view this email in your browser click on the following

Alternatively, you can also download any of the following clients on your email clients to view the secured email

[Help](#) | [Support](#) | [Downloads](#)

1. When you open the email, click View secured email in browser



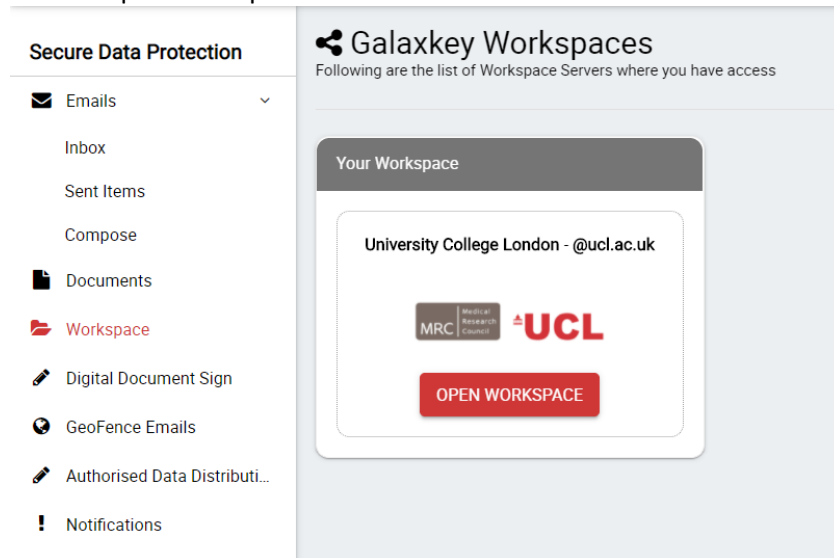
The screenshot shows a login form with the following fields: "Login ID" containing "n.tappenden@ucl.ac.uk", an empty "Password" field, a "Remember me" checkbox, and a red "LOGIN" button. A blue callout bubble points to the "Login ID" field with the text: "2. The website will open and you will be prompted to login". A pink callout bubble points to the "Password" field with the text: "If the user forgets their password, they will need to contact MRC CTU, their account will need to be re-set by IS and the email resent".



The screenshot shows an email header with the following details: "From: n.tappenden@ucl.ac.uk", "Subject:", "To:", and "Date: Friday, June 26, 2015". At the top right, there are buttons for "REPLY", "REPLY ALL", and "FORWARD". A blue callout bubble points to the "REPLY" button with the text: "3. The email will then open and can be replied to/forwarded from here".

### 6.1.3 USING GALAXKEY TO TRANSFER LARGE FILE – GALAXKEY WORKSPACE (SUPERSEDES GALAXKEY SECURE SHARE (GSS))

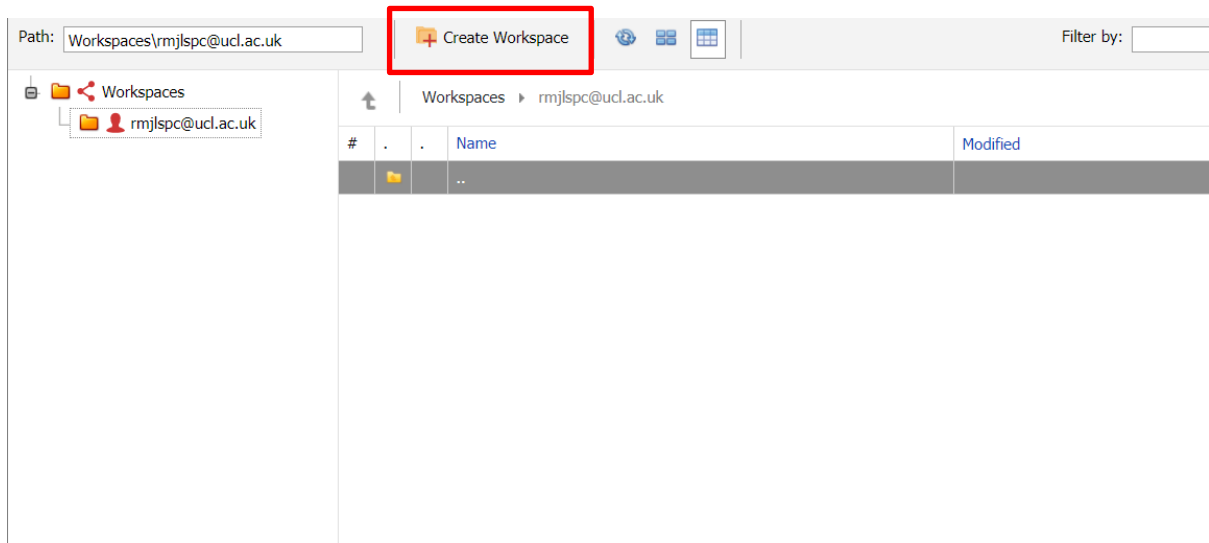
Navigate to: <https://manager.galaxkey.com/> and log in  
Choose "workspace" from the menu on the left  
Select "Open Workspace"



The screenshot shows the Galaxkey Workspaces interface. On the left is a sidebar menu titled "Secure Data Protection" with options: "Emails", "Inbox", "Sent Items", "Compose", "Documents", "Workspace", "Digital Document Sign", "GeoFence Emails", "Authorised Data Distributi...", and "Notifications". The main content area is titled "Galaxkey Workspaces" and contains the text "Following are the list of Workspace Servers where you have access". Below this, there is a card for "Your Workspace" for "University College London - @ucl.ac.uk". The card features the MRC Medical Research Council and UCL logos, and a red "OPEN WORKSPACE" button.

Once open, choose an identity on the left (you may be able to create using a trial inbox identity)

Use the “Create workspace” button at the top of the page to make a new workspace



Fill in the Name of the workspace and enter a description (these are mandatory fields).

A screenshot of the 'Workspace Configuration' dialog box. It is divided into two main sections: 'Workspace Details' and 'Attributes'.  
- 'Workspace Details':  
 - Name: A text input field with the placeholder 'Enter a unique Workspace Name'.  
 - Description: A larger text input field with the placeholder 'Enter a description for this workspace'.  
- 'Attributes':  
 - System Notifications: A group of checkboxes for 'Updated', 'Downloaded', 'Deleted', 'Added', and 'Viewed'.  
 - Enable time restriction: A checkbox followed by a dropdown menu.  
Below these sections is a 'Members and access rights' section. It features a toolbar with icons for edit, delete, add, refresh, search, user, notification, and check. A red box highlights a '+ NEW' button. Below the toolbar, it says 'No data to display'. At the bottom right, there are 'Save' and 'Cancel' buttons.

At this point you can add users who will be able to access this folder using the “New” button at the bottom. Assign them rights within the workspace as required.

Note: individuals need adding to each workspace individually with rights specific to that workspace

Member Editor ✕

Member Information

Email Identity:\*

File Access Rights

Write:  Delete:  Add:   
Download:  View Members:

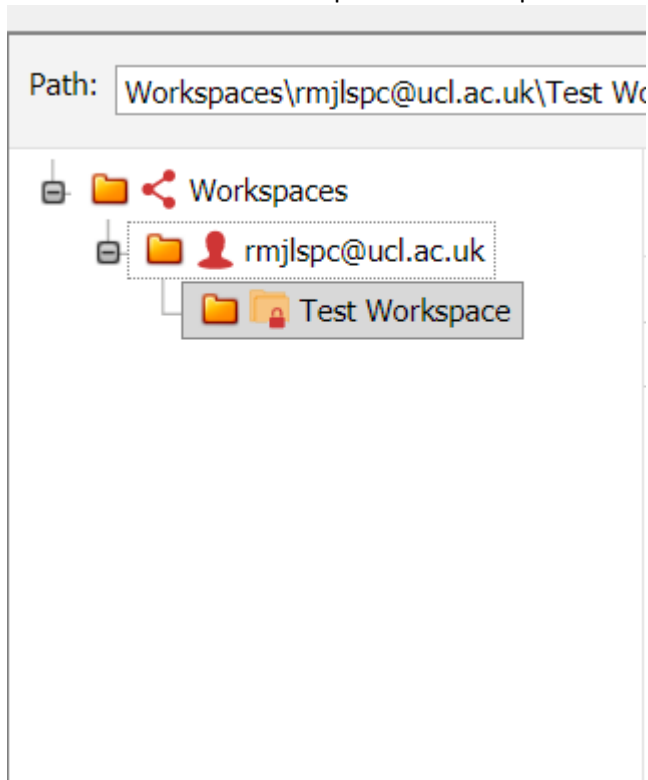
Reviewer Rights

Reviewer:

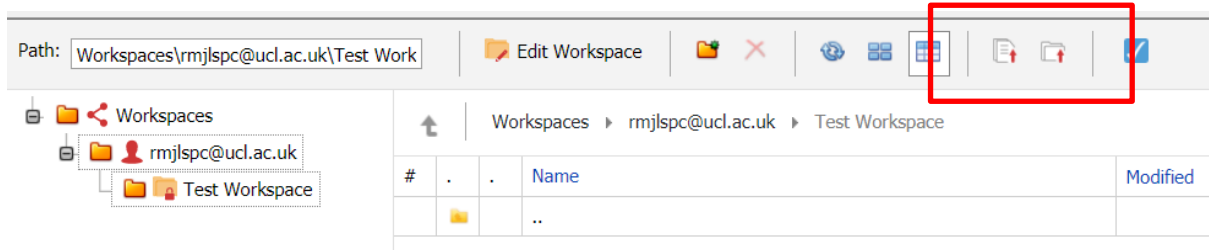
Administrative Rights

Manage Members:  System Notifications:

You will then see the workspace in the left panel



Click on the workspace to open it and use the upload file or folder options at the top of the screen to upload files into the workspace



#### 6.1.4 GALAXKEY WORKSPACE – FOR EXTERNAL USERS

When adding users to a workspace you can choose to send them an email automatically or manually.

When this is sent to a user who has not already had a Galaxkey account created i.e. an external user who has not been invited to take part in Galaxkey previously, then they will be prompted to create their account.

These credentials can then be used to log in to the Workspace or to access Galaxkey protected emails in the future.

The Workspace the user logs in to looks similar to the screenshots above, with no options for creating new folders.

## 6.2 7-ZIP

Whilst Galaxkey is the MRC CTU's preferred method of secure data exchange there are some instances in which is not practical to use e.g. when a collaborating institution does not support this. In such cases, all of the principles of secure exchange of participant personal data as described in this SOP remain applicable, information may be transferred using 7zip as described below.

Every PC at the MRC CTU has 7zip software that allows you to create zipped files. When you need to send information with study number plus any other indirect identifiers, the basic steps are to:

- Add it to a .zip file
  - NB the default file type for 7zip is a .7z file, however it does allow you to create .zip files also. This is the preference because it provides enhanced compatibility with other zipping software.
- Password protect the file. Ensure a strong password is used, for example a minimum of 8 characters, created using a mixture of upper and lower case letters, numbers and symbols. For more information, see the [UCL guidance on creating passwords](#).
- Send the password and the file in separate emails
- Click [here](#) for instructions on creating a secure .zip file using 7zip.

If a site or collaborator reported that they are unable to receive data via Galaxkey or 7zip this must be flagged with the IS department and the specifics of the issue should be reviewed with a view to finding an acceptable secure transfer mechanism that is in compliance with this SOP.