

Outline Data Collection, Collation and Security Procedure

1. Rationale: Leyton Orient Trust (LOT) collects, collates and evidences all participant information from all sessions and activities that it runs. This is done in partnership with our funders who require demonstration of evidence and for LOT's own internal marketing purposes.

2. Responsibility: In regards to the collection and collation of participant information, the day to day responsibility for this sits with the Philip Rudling, Deputy Chief Executive (DCEO) of LOT as well as the Lead Managers of each of the programmes. The DCEO and the Lead Managers receive paper registers which are then collated and updated to the appropriate platform by two LOT staff members - the Business Development Executive and a Development Coach - who data input and cross reference.

3. Usage: It should be noted that LOT currently uses a number of data platforms as follows:

- **Views** - for all Premier League (PL) and some EFL Trust (EFLT) activity
- **Upshot** - for some EFLT activity
- **Moodle** - for Waltham Forest College activity
- **Local Authority** - for activity relevant to their contracts

Once the information is on the relevant data platform, it is then assessed and used for project reports as appropriate. In addition to this stated usage, the information is also used in reports submitted to the **Quality Assurance and Improvement Committee** which oversees the process.

4. Security: In terms of security and data protection, LOT has an overall Data Protection Policy which is issued to all staff and volunteers. This ensures that:

- **LOT has an email and internet policy outlining how staff and volunteers should use such technology**
- **LOT is registered with the Information Commissioner's Office (ICO) and complies accordingly**
- **LOT uses the services of an IT Specialist who puts in place appropriate systems and checks on how all data that is used by the Trust is managed**
- **LOT has a fully functioning IT system which is integrated, networked and is security controlled**

In addition to the Data Protection Policy issued to staff and volunteers, LOT also has appropriate data protections policies in place for the management of information relating to children and young people, as well as vulnerable adults.

5. Access: LOT has a variety of users accessing the network which includes contracted employees, some sessional staff, students - and from September 2016 all LOT Trustees. To manage this access to data, LOT has in place the following:

- **Each authorised user has a user name and password which they set and which expires every 6 months**
- **Each authorised user has their own "H Drive" on the network which is only accessible through their password protected log in**
- **Each authorised user has an official email address linked to Microsoft Outlook**
- **Whilst each authorised user has access to the shared "H Drive" this is restricted based on the type of user and seniority within the organisation**
- **Only LOT's CEO has full access to all aspects of the Shared Drive**
- **Contracted employees are also given rights to access the system remotely**

6. Storage: LOT uses two servers which are interconnected and stored in a server room in a secure area of the building they occupy. To enter the server room, two locked doors need to be opened by building staff. LOT uses Data Barracks to store and back up all data virtually and this takes place every evening. The IT Specialist is the administrator of the system and is the only one that has access to the whole system.

7. Sharing Data: Currently no data that LOT collects is shared with any third party organisation - including Leyton Orient Football Club. LOT has in place the appropriate policies for the sharing of a child, young person and/or vulnerable adult's data where this would be required. Moreover, the Club collects data independently through their own **Junior Supporters Club** - and which appropriate LOT participants are encouraged to be part of.

Reviewed & Updated: April 2016

LOT will review this Outline Data Collection, Collation and Security Procedure and good practice at least annually.

Employee Data Protection Policy

Personal information regarding all employees will be kept strictly confidential and any records held will be the responsibility of **Philip Rudling, Deputy Chief Executive**, LOT's Data Protection Officer, and protected by the Data Protection Act 1998.

In the course of your work you may come into contact with or use confidential information about employees, clients and customers, for example their names and home addresses. The Data Protection Act 1998 contains principles affecting employee and other personal records. Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data, for example employee personnel files that form part of a structured filing system.

The purpose of LOT's data protection rules is to ensure you do not breach the Act. If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from LOT's Data Protection Officer.

You should be aware that you could be criminally liable if you knowingly or recklessly disclose personal data in breach of the Act. A serious breach of data protection is also a disciplinary offence and will be dealt with under LOT's disciplinary procedures. If you access another employee's personnel records without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal.

The data protection principles: There are eight data protection principles that are central to the Act. LOT and all its employees must comply with these principles at all times in its information-handling practices. In brief, the principles say that personal data must be:

1. Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data

The conditions are either that the employee has given consent to the processing, or the processing is necessary for the various purposes set out in the Act. Sensitive personal data may only be processed with the explicit consent of the employee and consists of information relating to:

- Race or ethnic origin
- Political opinions and trade union membership
- Religious or other beliefs
- Physical or mental health or condition
- Sexual life
- Criminal offences, both committed and alleged

2. Obtained only for one or more specified and lawful purposes, and not processed in a manner incompatible with those purposes

3. Adequate, relevant and not excessive

LOT will review personnel files on an annual basis to ensure they do not contain a backlog of out-of-date information and to check there are sound business reasons requiring information to continue to be held.

4. Accurate and kept up-to-date

If your personal information changes, for example you change address, you must inform your line manager as soon as practicable by submitting a newly completed employee data form so that your records can be updated. LOT cannot be held responsible for any errors unless you have notified LOT of the relevant change/s on the employee data form.

5. Not kept for longer than is necessary

LOT will keep personnel files for no longer than six years after termination of employment. Different categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data, which LOT decides it does not need to hold for a period of time, will be destroyed after one year. Data relating to unsuccessful job applicants will only be retained for a period of one year.

6. Processed in accordance with the rights of employees under the Act

7. Secure, technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, data

Personnel files are confidential and are stored in locked filing cabinets. Only authorised staff have access to these files. Files will not be removed from their normal place of storage without good reason. Data stored on CD-ROM or other removable media will be kept in locked filing cabinets. Data held on computer will be stored confidentially by means of password protection, encryption or coding and again only

authorised employees have access to that data. LOT has network backup procedures to ensure that data on computer cannot be accidentally lost or destroyed.

8. Not transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the processing of personal data

Your consent to personal information being held: LOT holds personal data about you and, by signing your Statement of Terms and Conditions of Employment you have consented to that data being processed by LOT. Agreement to LOT processing your personal data is a condition of your employment.

LOT also holds limited sensitive personal data about its employees and, by signing your Statement of Terms and Conditions of Employment, you give your explicit consent to LOT holding and processing that data, for example sickness absence records, health needs and equal opportunities monitoring data.

Your right to access personal information: You have the right, on request, to receive a copy of the personal information that LOT holds about you, including your personnel file, and to demand that any inaccurate data be corrected or removed. You have the right on request:

- To be told by LOT whether and for what purpose personal data about you is being processed
- To be given a description of the data and the recipients to whom it may be disclosed
- To have communicated in an intelligible form the personal data concerned, and any information available as to the source of the data
- To be informed of the logic involved in computerised decision-making

Upon request, LOT will provide you with a statement regarding the personal data held about you. This will state all the types of personal data LOT holds and processes about you and the reasons for which they are processed.

If you wish to access a copy of any personal data being held about you, you must make a written request for this and LOT reserves the right to charge you a fee of up to £10. To make a request, please complete a Personal Data Subject Access Request Form, which can be obtained from the Data Protection Officer.

If you wish to make a complaint that these rules are not being followed in respect of personal data LOT holds about you, you should raise the matter with the Data Protection Officer. If the matter is not resolved to your satisfaction, it should be raised as a formal grievance under LOT's grievance procedure.

Your obligations in relation to personal information: You should ensure you comply with the following guidelines at all times:

- Do not give out confidential personal information except to the data subject. In particular, it should not be given to someone from the same family or to any other unauthorised third party unless the data subject has given their explicit consent to this
- Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone
- Only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail
- If you receive a request for personal information about another employee, you should forward this to the Chief Executive of LOT who will be responsible for dealing with such requests
- Ensure any personal data you hold is kept securely, either in a locked filing cabinet or, if computerised, it is password protected

Compliance with the Act is your responsibility. If you have any questions or concerns about the interpretation of these rules, please discuss this with LOT's Data Protection Officer.

Procedure for the Management of Records, Confidentiality & Sharing of Information

Policy statement: LOT expects the utmost confidentiality of all records relating to its safeguarding work with children and young people. LOT's staff members and volunteers will come into contact with personal and sensitive details about the lives of the children and young people with whom they will work, or who are in their care. None of this information - or information about a child or young person's families - should ever be the subject of gossip, or be passed on to anyone else without good cause or reason. Great care should be taken to ensure that when cases do have to be discussed with colleagues that the details cannot be overheard by anyone else. For the avoidance of doubt, information of a confidential nature should only be communicated on a need-to-know basis and - in most circumstances - with the consent of the child or young person and/or their families.

When reaching a decision about the disclosure of personal information the following three core ethical principles will be upheld:

1. All individuals have a fundamental right to the confidentiality and privacy of information related to their health and social care
2. All individuals have a right to control access to and the disclosure of their own health and social care information by giving, withholding or withdrawing consent
3. For any disclosure of confidential information, those involved should always have regard to its necessity, proportionality and any risks attached to it

However, not-with-standing the above, LOT staff members and volunteers should always be clear that in circumstances where there are concerns about an individual's safety and welfare - or the safety of others - they will always be required to pass on information that may have been received in confidence. In these circumstances, any information should be passed either to the staff members or volunteers Line Manager, or Philip Rudling, Deputy Chief Executive, LOT's Designated Safeguarding Officer.

LOT's Data Protection Policy: The under-pinning principles of LOT's responsibility in relation to the gathering, storage, usage and sharing of personal information is in line with the requirements of the Data Protection Act 1998.

Introduction: In the course of a staff members or volunteers work with LOT, they will come into contact with, or use, confidential information relating to children and young people. The Data Protection Act 1998 (the Act) contains principles affecting children and young people's information and personal records. Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data e.g. children and young people's information files that form part of a structured filing system. The purpose of these rules is to ensure that no LOT staff member or volunteer breaches the Act. If a staff member or volunteer is in any doubt about what can or cannot be disclosed and to whom, then the default position is not to disclose any personal information until advice has been provided by LOT's Data Protection Officer.

Under the Act, all LOT staff members and volunteers are personally accountable for their actions and can be held criminally liable if they knowingly, or recklessly, breach it. Any serious breach of data protection legislation will also be regarded as misconduct and will be dealt with under the Company's disciplinary procedures. Any access of a children and young people's records - without authority - constitutes a gross misconduct offence and could lead to summary dismissal or termination of a volunteering agreement.

The data protection principles: There are eight data protection principles that are central to the Act. LOT and all its staff members and volunteers must comply with these principles at all times in its information-handling practices. **In brief, the principles say that personal data must be:**

1. **Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data - and additional conditions are met in relation to sensitive personal data.** The conditions are either that the individual has given consent to the processing, or the processing is necessary for the various purposes set out in the Act.
2. **Obtained only for one or more specified and lawful purposes, and not processed in a manner incompatible with those purposes.**
3. **Adequate, relevant and not excessive.** LOT will only collect essential personal details of children and young people for whom it provides services or activities to. **Essential joining information will include:**
 - The name, address and contact number of all children and young people - and where appropriate their carers, advocates or next of kin
 - Any medical and health issues or particular requirements
 - Contact with other professionals or agencies, if any.

Procedure for the Management of Records, Confidentiality & Sharing of Information continued...

LOT will also keep records which reflect the child or young person's ongoing engagement with the organisation. This will include records on attendance, activities participated in and any incidents, accidents and/or near misses that occur.

4. **Accurate and kept up-to-date.** Where personal information relating to a child or young person changes, LOT will need to be informed promptly by so that appropriate records can be updated. LOT cannot be held responsible for any errors unless they organisation has been notified of the relevant change.
5. **Not kept for longer than is necessary:** LOT will dispose of children and young person's information within the timescales that are in keeping with the requirements of the Data Protection Act.
6. **Processed in accordance with the rights of children and young people under the Act.** The uses that LOT anticipates that collected personal data will be used for can include such things as:
 - To better manage, plan and improve the services and/or activities provided
 - To help train and teach LOT staff members and volunteers
 - To help with research, but only with the child or young person's agreement
 - To provide statistics about LOT services and activities delivered by the organisation - whilst ensuring that personal information will not be disclosed or used in this way and will never be shared with anyone, other than in the circumstances set out below
7. **Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data:** All written records will be stored in a secure location and accessed by authorised personnel only. Electronic records held on computers will also be appropriately secured by way of password protection and restricted access.
8. **Not transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the processing of personal data.**

As far as the sharing of confidential information and management records are concerned, LOT will adhere to the following standards and procedures:

Sharing confidential information within the organisation: Information will only be shared within LOT on a need to know basis only. LOT line managers will have access to information to check that records are being made and maintained appropriately and to enable them to identify patterns of behaviour emerging from incident reporting.

Sharing confidential information with children and young people, carers & advocates: Children and young people - as well as their carers and advocates - will always be told how information will be used before they are asked to provide it and will be given an opportunity to discuss such uses. Explanations of how information will be used will always be communicated in a way which is clearly understood - and alternative means of communication will be used where necessary.

When a child or young person's information needs to be shared - **e.g.** in the case of an emergency or of suspected abuse, the child or young person and/or their carer or advocate will be told what information was shared as soon as possible, whilst ensuring that this does not expose the child or young person to further risk of harm.

Sharing confidential information with external agencies: While information about children and young people is confidential, it may need to be disclosed to external agencies to ensure the care and safety of an individual, or of others, or where a crime is suspected. Children and young people, in normal circumstances, can expect to see any information held by LOT about them - and LOT will take steps to inform them of this right to access their information. This right will apply to both paper and electronic records - and will include access to care records - unless any of the reasons for limiting access set out below apply.

Access will be provided, if requested, to the child or young person, and, with their consent to another person acting on their behalf. LOT will, where it is possible and reasonable, require all such requests to access records to be made in writing. Regardless of how a request is received LOT will maintain records or all requests received and their outcomes.

Where a request to access of a child or young person's records has to be limited, this decision will always be recorded. Circumstances in which limited access may be applied could include where any part of a record contains confidential information about other people; or information was provided by another person or agency - such as doctor or other professional - and their permission has not been obtained. There may also be a requirement to limit access to information in circumstances where a care professional thinks access would cause serious harm to the child or young person's, or someone else's physical or mental well-being.

Procedure for the Management of Records, Confidentiality & Sharing of Information continued...

LOT's staff members and volunteer's obligations in relation to personal information: Any staff member or volunteer - who as part of their job duties and responsibilities - are required to collect personal information about children and young people, must comply with this policy. This includes ensuring the information is processed in accordance with the Act; is only processed for the purposes for which it is held; is kept secure; and is not kept for longer than necessary. ***The following guidelines must be complied with at all times:***

All LOT staff members and volunteers must:

- Never disclose confidential personal information to anyone except the data subject or to a person authorised by the data subject. In particular, unless the data subject has given their explicit prior written consent, personal information should not be:
 - a) Given to someone from the same family
 - b) Passed to any other unauthorised third party
 - c) Placed on the Company's website
 - d) Posted on the Internet in any form
- Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone
- Where LOT provides staff members and volunteers with code words or passwords to be used before releasing personal information - e.g. by telephone, always strictly follow the Company's requirements in this regard
- Only transmit personal information between locations by fax or e-mail if a secure network is in place - e.g. a confidential fax machine or encryption is used for e-mail
- Forward all requests for personal information about a child or young person to LOT's Data Protection Officer without delay
- Keep all personal data securely, either in a locked filing cabinet or, if computerised, by it being password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons
- Not access any child or young person's records without authority as this will be treated as gross misconduct and it is a criminal offence
- Never write down (in electronic or hard copy form) opinions or facts concerning a data subject which it would be inappropriate to share with that data subject
- Never remove personal information from the workplace with the intention of processing it elsewhere, unless this is necessary to enable you to carry out your job duties and has been prior authorised by a line manager
- Ensure that, when working on personal information as part of designated job duties when away from LOT's workplace - and with the prior authorisation of a line manager – the terms of this policy and the Act continue to be observed at all times, particularly in matters of data security
- Ensure that hard copy personal information is disposed of securely - e.g. by cross-shredding
- Remember that compliance with the Act is each individual's personal responsibility. If staff members or volunteers ever have any questions or concerns about the interpretation of these rules, they should immediately contact LOT's Data Protection Officer.

Reviewed & Updated: April 2016

LOT will review this Procedure for the Management of Records, Confidentiality & Sharing of Information and good practice at least annually.

Procedure for the Management of Records, Confidentiality & Sharing of Information

Policy statement: LOT expects the utmost confidentiality of all records relating to its safeguarding work with vulnerable adults. LOT's staff members and volunteers will come into contact with personal and sensitive details about the lives of the vulnerable adults with whom they will work, or who are in their care. None of this information - or information about a vulnerable adult's families - should ever be the subject of gossip, or be passed on to anyone else without good cause or reason. Great care should be taken to ensure that when cases do have to be discussed with colleagues that the details cannot be overheard by anyone else. For the avoidance of doubt, information of a confidential nature should only be communicated on a need-to-know basis and - in most circumstances - with the consent of the vulnerable adult.

When reaching a decision about the disclosure of personal information the following three core ethical principles will be upheld:

1. All individuals have a fundamental right to the confidentiality and privacy of information related to their health and social care
2. All individuals have a right to control access to and the disclosure of their own health and social care information by giving, withholding or withdrawing consent
3. For any disclosure of confidential information, those involved should always have regard to its necessity, proportionality and any risks attached to it

However, not-with-standing the above, LOT staff members and volunteers should always be clear that in circumstances where there are concerns about an individual's safety and welfare - or the safety of others - they will always be required to pass on information that may have been received in confidence. In these circumstances, any information should be passed either to the staff members or volunteers Line Manager, or Philip Rudling, Chief Executive, LOT's Nominated Manager.

LOT's Data Protection Policy: The under-pinning principles of LOT's responsibility in relation to the gathering, storage, usage and sharing of personal information is in line with the requirements of the Data Protection Act 1998.

Introduction: In the course of a staff members or volunteers work with LOT, they will come into contact with, or use, confidential information relating to vulnerable adults. The Data Protection Act 1998 (the Act) contains principles affecting vulnerable adult's information and personal records. Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data e.g. vulnerable adult's information files that form part of a structured filing system. The purpose of these rules is to ensure that no LOT staff member or volunteer breaches the Act. If a staff member or volunteer is in any doubt about what can or cannot be disclosed and to whom, then the default position is not to disclose any personal information until advice has been provided by LOT's Data Protection Officer.

Under the Act, all LOT staff members and volunteers are personally accountable for their actions and can be held criminally liable if they knowingly, or recklessly, breach it. Any serious breach of data protection legislation will also be regarded as misconduct and will be dealt with under the Company's disciplinary procedures. Any access of a vulnerable adult's records - without authority - constitutes a gross misconduct offence and could lead to summary dismissal or termination of a volunteering agreement.

The data protection principles: There are eight data protection principles that are central to the Act. LOT and all its staff members and volunteers must comply with these principles at all times in its information-handling practices. **In brief, the principles say that personal data must be:**

1. **Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data - and additional conditions are met in relation to sensitive personal data.** The conditions are either that the individual has given consent to the processing, or the processing is necessary for the various purposes set out in the Act.
2. **Obtained only for one or more specified and lawful purposes, and not processed in a manner incompatible with those purposes.**
3. **Adequate, relevant and not excessive.** LOT will only collect essential personal details of vulnerable adults for whom it provides services or activities to. **Essential joining information will include:**
 - The name, address and contact number of all vulnerable adults - and where appropriate their carers, advocates or next of kin
 - Any medical and health issues or particular requirements
 - Contact with other professionals or agencies, if any.

LOT will also keep records which reflect the vulnerable adult's ongoing engagement with the organisation. This will include records on attendance, activities participated in and any incidents, accidents and/or near misses that occur.

Procedure for the Management of Records, Confidentiality & Sharing of Information continued...

4. **Accurate and kept up-to-date.** Where personal information relating to a vulnerable adult changes, LOT will need to be informed promptly by so that appropriate records can be updated. LOT cannot be held responsible for any errors unless they organisation has been notified of the relevant change.
5. **Not kept for longer than is necessary:** LOT will dispose of vulnerable adult's information within the timescales that are in keeping with the requirements of the Data Protection Act.
6. **Processed in accordance with the rights of vulnerable adults under the Act.** The uses that LOT anticipates that collected will be used for can include such things as:
 - To better manage, plan and improve the services and/or activities provided
 - To help train and teach LOT staff members and volunteers
 - To help with research, but only with the vulnerable adult's agreement
 - To provide statistics about LOT services and activities delivered by the organisation - whilst ensuring that personal information will not be disclosed or used in this way and will never be shared with anyone, other than in the circumstances set out below
7. **Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data:** All written records will be stored in a secure location and accessed by authorised personnel only. Electronic records held on computers will also be appropriately secured by way of password protection and restricted access.
8. **Not transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the processing of personal data.**

As far as the sharing of confidential information and management records are concerned, LOT will adhere to the following standards and procedures:

Sharing confidential information within the organisation: Information will only be shared within LOT on a need to know basis only. LOT line managers will have access to information to check that records are being made and maintained appropriately and to enable them to identify patterns of behaviour emerging from incident reporting.

Sharing confidential information with vulnerable adults, carers & advocates: Vulnerable adults - as well as their carers and advocates - will always be told how information will be used before they are asked to provide it and will be given an opportunity to discuss such uses. Explanations of how information will be used will always be communicated in a way which is clearly understood - and alternative means of communication will be used where necessary.

When a vulnerable adult's information needs to be shared - **e.g.** in the case of an emergency or of suspected abuse, the vulnerable adult and/or their carer or advocate will be told what information was shared as soon as possible, whilst ensuring that this does not expose the vulnerable adult to further risk of harm.

Sharing confidential information with external agencies: While information about vulnerable adults is confidential, it may need to be disclosed to external agencies to ensure the care and safety of an individual, or of others, or where a crime is suspected. Vulnerable adults, in normal circumstances, can expect to see any information held by LOT about them - and LOT will take steps to inform them of this right to access their information. This right will apply to both paper and electronic records - and will include access to care records - unless any of the reasons for limiting access set out below apply.

Access will be provided, if requested, to the vulnerable adult, and, with their consent to another person acting on their behalf. LOT will, where it is possible and reasonable, require all such requests to access records to be made in writing. Regardless of how a request is received LOT will maintain records or all requests received and their outcomes.

Where a request to access of a vulnerable adult's records has to be limited, this decision will always be recorded. Circumstances in which limited access may be applied could include where any part of a record contains confidential information about other people; or information was provided by another person or agency - such as doctor or other professional - and their permission has not been obtained. There may also be a requirement to limit access to information in circumstances where a care professional thinks access would cause serious harm to the vulnerable adult's, or someone else's physical or mental well-being.

LOT's staff members and volunteer's obligations in relation to personal information: Any staff member or volunteer - who as part of their job duties and responsibilities - are required to collect personal information about vulnerable adults, must comply with this policy. This includes ensuring the information is processed in accordance with the Act; is only processed for the purposes for which it is held; is kept secure; and is not kept for longer than necessary. **The following guidelines must be complied with at all times:**

Procedure for the Management of Records, Confidentiality & Sharing of Information continued...

All LOT staff members and volunteers must:

- Never disclose confidential personal information to anyone except the data subject or to a person authorised by the data subject. In particular, unless the data subject has given their explicit prior written consent, personal information should not be:
 - a) Given to someone from the same family
 - b) Passed to any other unauthorised third party
 - c) Placed on the Company's website
 - d) Posted on the Internet in any form
- Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone
- Where LOT provides staff members and volunteers with code words or passwords to be used before releasing personal information - e.g. by telephone, always strictly follow the Company's requirements in this regard
- Only transmit personal information between locations by fax or e-mail if a secure network is in place - e.g. a confidential fax machine or encryption is used for e-mail
- Forward all requests for personal information about a vulnerable adult to LOT's Data Protection Officer without delay
- Keep all personal data securely, either in a locked filing cabinet or, if computerised, by it being password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons
- Not access any vulnerable adult's records without authority as this will be treated as gross misconduct and it is a criminal offence
- Never write down (in electronic or hard copy form) opinions or facts concerning a data subject which it would be inappropriate to share with that data subject
- Never remove personal information from the workplace with the intention of processing it elsewhere, unless this is necessary to enable you to carry out your job duties and has been prior authorised by a line manager
- Ensure that, when working on personal information as part of designated job duties when away from LOT's workplace - and with the prior authorisation of a line manager – the terms of this policy and the Act continue to be observed at all times, particularly in matters of data security
- Ensure that hard copy personal information is disposed of securely - e.g. by cross-shredded
- Remember that compliance with the Act is each individual's personal responsibility. If staff members or volunteers ever have any questions or concerns about the interpretation of these rules, they should immediately contact LOT's Data Protection Officer.

An example of LOT's Essential Service User Information Form can be found in the appendix section of this Vulnerable Adult Safeguarding Policies and Procedures Handbook and further copies can be obtained from LOT's Designated Safeguarding Officer.

Reviewed & Updated: April 2016

LOT will review this Procedure for the Management of Records, Confidentiality & Sharing of Information and good practice at least annually.