

General Data Protection Regulation Policy

Version:	9
Name & job title of policy owner	Julia Ward Quality manager
Date approved by SMT:	16 th January 2020
Next review date:	June 2021

Contents

Part One - Data Protection Principles.....	4
Principle 1: Lawfulness, fairness and transparency	4
Principle 2: Purpose limitation	5
Principle 3: Data minimisation	5
Principle 4: Accuracy.....	5
Principle 5: Storage limitation	5
Principle 6: Integrity and confidentiality	6
Principle 7: Accountability	6
Part Two – The rights of individuals.....	8
2.1 Right to be informed.....	8
2.2 Right of access.....	8
2.2.1 Children and subject access requests.....	8
2.2.2 Subject access procedures.....	9
2.3 Right to rectification	9
2.3.1 Opinions	9
2.3.2 What we will do if we are satisfied the data is accurate	9
2.3.4 Informing other organisations.....	9
2.4 Right to erasure (also known as the ‘right to be forgotten’).....	9
2.4.1 Who we tell about personal data that has been erased.....	10
2.4.2 When does the right to erasure not apply?	10
2.5 Right to restrict processing.....	10
2.5.1 When does the right to restrict processing apply?	10
2.5.2 What we do with restricted data	11
2.5.3 Who we will tell about the restriction of personal data?.....	11
2.5.4 When can we lift the restriction?	11
2.6 Right to data portability	11
2.7 Right to object.....	11
2.7.1 Direct marketing	12
2.7.2 Public task or legitimate interests.....	12
2.7.3 Research purposes.....	12
2.7.4 Action we will take when we receive a right to object.....	12
2.8 Rights related to automated decision making including profiling	12
3. How we respond to requests	12
3.1 Fees	12
3.2 Timescales for responding to requests	13
3.3 Confirming identity.....	13
4. Complaints	13
Part three - information security	14
Records.....	14
3.1 Paper records.....	14
3.2 Electronic records	14
3.3 Clear desk and clear screen policy	15
3.3.1 Clear desk	15
3.3.2 Clear screen policy	16
3.5 Use of email	16
3.6 Use of telephone, fax, email and internet	17
3.6.1 Telephone (landline and mobile)	17
3.6.2 Telephone voicemail	18
3.6.3 Text/messaging services	18
3.6.4 Fax	18
3.6.5 Internet.....	18
3.6 Post.....	18
3.6.1 Outgoing post	19
3.6.2 Incoming post	19

3.7	Physical security.....	19
3.7.1	Building access control.....	19
3.7.2	Dealing with visitors	19
3.7.3	Rooms with secure access	20
3.7.4	Locking/unlocking	20
3.7.5	Closed circuit television (CCTV).....	20
3.8	IT security	23
3.8.1	Physical security of IT equipment	23
3.8.2	Network security.....	23
3.8.3	Email filters.....	23
3.8.4	Device hardening	23
3.9	Access controls.....	24
3.9.1	Network log-in	24
3.9.2	Log-in/passwords.....	24
3.9.3	Wi-Fi.....	25
3.9.4	Guest access to the server	25
3.9.5	Remote access to the server	25
3.9.6	Network monitoring.....	25
3.10	SharePoint	25
3.11	Third party applications/databases externally hosted	26
3.12	Back-up	26
3.13	Destruction and disposal of personal data.....	26
3.13.1	Data Held Electronically	26
3.13.2	IT Asset Disposal.....	26
3.13.3	Asset Disposal Process.....	26
3.13.4	Process to Dispose of ICT Assets.....	27
Part four – management of personal data breaches		28
4.1	Personal data breach management.....	28
4.2	Notification to the ICO	28
4.3	How to notify the ICO	28
4.4	Timescale for reporting notifiable breaches to the ICO.....	29
4.5	Data processors.....	29
4.6	Telling individuals (data subjects) about a breach	29
Part five - Responsibilities.....		30
5.1	Board of trustees	30
5.2	Senior management team	30
5.3	Chief executive officer	30
5.4	Directors	30
5.5	Data Protection Officer	30
5.6	Human resources assistant.....	30
5.7	Managers.....	31
5.8	Communications manager.....	31
5.9	All staff	31
6.	Specialist and competent person advice	31
7.	Implementation and monitoring.....	31
7.1	Implementation.....	31
7.2	Process for monitoring implementation and effectiveness	31
8.	References.....	32
9.	Related documents.....	32
10.	Definitions	32
11.	Version control.....	33
Appendix A - ICO certificate of registration		34
Appendix B - Information retention schedule 2019.....		34
Appendix C - Data protection privacy impact screening template		34
Appendix D - Data protection impact assessment template		34
Appendix E - Legitimate interests' assessment template.....		34
Appendix F - ICO Report a personal data breach template		34

Introduction

This policy details how LifeLine Community Projects (LifeLine) aims to ensure that personal data about beneficiaries, staff, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and other relevant regulations, codes of practice and guidance.

LifeLine processes personal data as a data controller. This means as a controller we determine the purposes and the means of processing personal data. We are also responsible for processing personal data on behalf of data controllers and as such are also data processors. We have specific legal obligations under the GDPR as a data controller and in our role of data processor.

LifeLine is registered as a data controller with the Information Commissioner’s Office (ICO). Our registration number is Z6591927. The current registration period runs from 26th March 2002 to 25th March 2020 – see appendix A for a copy of LifeLine’s ICO registration certificate. Registration is renewed annually, or as otherwise legally required.

Part One - Data Protection Principles

At the heart of LifeLine’s approach to processing personal data are the seven key principles of the GDPR. These are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

The sections below detail the systems LifeLine has in place to meet the seven key principles.

Principle 1: Lawfulness, fairness and transparency

Lawfulness

Under the GDPR, the requirements for the lawful bases for processing information are:

Consent	The individual has given clear consent for LifeLine to process their personal data for a specific purpose.
Contract	The processing is necessary for a contract LifeLine has with an individual, or because an individual has asked LifeLine to take specific steps before entering into a contract.
Legal obligation	The processing is necessary for LifeLine to comply with the law (not including contractual obligations).
Vital interests	The processing is necessary to protect someone’s life.
Public task	The processing is necessary for LifeLine to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
Legitimate interests	The processing is necessary for LifeLine’s legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests.

How LifeLine Projects meets this principle:

- We will only collect and use personal data when we have identified a valid and appropriate lawful basis for processing.
- We conducted a GDPR audit in 2018 and recorded the lawful bases for all existing data processing activities. Since the audit, we have produced a Record of Processing Activities (RoPA). The RoPA will be reviewed at least annually.
- For new contracts, we will identify and document the lawful basis in the RoPA before we begin processing. The basis will be identified at the contract implementation stage.

- We include information about the purposes of the processing and the lawful basis for the processing in our privacy notices.
- We have included the conditions for processing special category and criminal offence data in the GDPR audit document.

Fairness

We will only use personal data in a way that is fair and in ways that people would reasonably expect. We will not process data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.

Transparency

We will be clear, open and honest with people from the start about how we will use their personal data and will comply with the transparency obligations of the right to be informed - see 2.1.

We will tell individuals about how we process personal data in clear and plain language and in ways that are easily accessible and easy to understand.

Principle 2: Purpose limitation

LifeLine will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. We record these purposes in the GDPR audit document and specify them in our privacy notices. This information is reviewed regularly.

We will only use the personal data for a new purpose if it is compatible with our original purpose, we get consent, or have a clear basis in law.

Principle 3: Data minimisation

We will identify the minimum amount of personal data we need to fulfil our specified purposes for collecting it. We review the data we hold in line with our Information Retention Schedule - see appendix B, and delete anything we don't need.

Principle 4: Accuracy

LifeLine takes reasonable steps to ensure the accuracy of the personal data we create, or data that is provided by someone else. We will correct or delete inaccurate data. We seek clarification of authenticity and accuracy at the point of data collection. We generally only collect personal data directly from individuals. We have appropriate processes in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary. For example, LifeLine has progress review processes in place when working with beneficiaries on some of its contracts. Review meetings provide opportunities to correct and update personal data e.g. change of address or telephone number. Similarly, HR periodically seeks updated information from staff so that employee details on the HR database can be kept up to date. Staff, beneficiaries and other stakeholders always sign to confirm that the personal data they provide is a true and accurate to the best of their knowledge.

However, this can become more complicated when personal data is added to, commented upon, or predictions are made based on a person's professional opinion. Where this applies, our records will clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.

We comply with the individual's right to rectification - see 2.3, and carefully consider any challenges to the accuracy of the personal data.

Principle 5: Storage limitation

LifeLine will not keep personal data for longer than it is needed and we will ensure we are able to justify, based on the purposes for holding the data, how long we keep personal data.

To comply with this requirement, we:

- review the length of time personal data is retained
- consider the purpose(s) we hold the personal data for in deciding whether (and for how long) to retain it
- securely delete personal data that is no longer needed
- update, archive and securely delete personal data if it goes out of date.

Retention periods will depend on what the information is used for, the purpose for which it was obtained and its nature. Some information retained by LifeLine is determined by contract requirements (i.e. funder's state the retention period for which documentation has to be retained). If it continues to be necessary to hold the data for other reasons (such as compliance with employment law), then we will retain it for as long as that reason applies.

Marketing and promotional materials containing personal information that need to be retained for LifeLine's historical purposes will be retained indefinitely. Information with only a short-term value will be deleted within days, for example, CCTV images.

Retention periods also take into account legal and business-sector requirements and professional guidelines such as information needed for income tax and audit purposes, or information on aspects of health and safety. Where LifeLine retains personal data to comply with requirements such as these, it will not be considered to have kept the information for longer than necessary. Anonymised records (personal details removed) can be retained for business performance and comparison reasons and have no restrictions.

LifeLine reviews personal data held, and deletes anything no longer needed. Information that does not need to be accessed regularly, but which still needs to be retained, will be archived securely.

LifeLine has a contract closure process that is implemented through scorecard meetings. A contract closure document records activity associated with closure and includes the details of the retention period for the contract, the identification of paper and/or electronic records to be retained, the structure of the electronic filing archive and where relevant, the process for sending paper documentation to off-site archive storage. The process also includes actions to be taken where services are transferred to another provider, and where there is a requirement for original records to be returned to the funder at the end of the contract period. Responsibility for each stage of the archive process is allocated to named staff and recorded on the contract closure record.

The GDPR does not specify retention periods. Therefore, unless otherwise stated, LifeLine's minimum retention period is 6 years. This is based on the 6-year time limit within which legal proceedings must be commenced as laid down under the Limitation Act 1980. The minimum retention period only applies where there is no stated contractual requirement or legislative authority.

Principle 6: Integrity and confidentiality

LifeLine has appropriate security measures in place to prevent personal data being accidentally or deliberately compromised.

Every aspect of our processing activities is covered, including cybersecurity. This means the security measures we have in place seek to ensure that:

- the data can be accessed, altered, disclosed or deleted only by those authorised to do so (and that those people only act within the scope of the authority given to them)
- the data we hold is accurate and complete in relation to why we are processing it
- the data remains accessible and usable, i.e. if personal data is accidentally lost, altered or destroyed, we should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

These are known as 'confidentiality, integrity and availability' and under the GDPR, they form part of our obligations.

Full details of information security arrangements can be found in part three of this policy.

Principle 7: Accountability

One of the biggest changes introduced by the GDPR is around accountability – a new data protection principle that says organisations are responsible for, and must be able to demonstrate compliance with the other principles.

LifeLine is proactive about data protection and we have taken the following measures to demonstrate compliance with the accountability principle. We have:

- Updated our data protection, information security and associated policies and procedures in line with the requirements of GDPR.
- Updated privacy notices.
- Introduced a screening tool, see appendix C, for use during contract implementation stage to help us decide if we need to complete a full data protection impact assessment.
- Taken a 'data protection by design and default' approach and introduced a system for completing data protection impact assessments (DPIAs), see appendix D, for processing data that is likely to result in a high risk to individuals. LifeLine's data audit completed in May 2018, and subsequent RoPA, has not highlighted any activities that require the mandatory completion of DPIAs, or any processing that poses a high risk to individuals.
- Implemented a process for issuing written contracts to organisations who process data on our behalf.
- Reviewed our security measures to ensure they are appropriate and up to date.
- Updated our procedures for investigating, recording and, where necessary, reporting personal data breaches to the ICO – see part 4, management of personal data breaches.
- Identified GDPR training for staff.

We review our accountability measures at appropriate intervals and, where necessary, update the measures we have in place.

Part Two – The rights of individuals

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

The sections below detail the systems LifeLine has in place to protect the rights of individuals.

2.1 Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

We provide individuals with privacy information at the time we obtain their data. This can be in the form of privacy notices published on our websites, or within documents that we use to gather personal data.

We endeavour to provide people with privacy information in a way that is concise, transparent, intelligible and easily accessible. We use clear and plain language to achieve this.

We regularly review, and where necessary, update our privacy information.

Where it applies, we will bring any new uses of an individual's personal data to their attention before we start the processing.

2.2 Right of access

The reason for allowing individuals to access their personal data is so that they are aware of, and can verify the lawfulness of the processing.

Individuals have the right to obtain confirmation that their data is being processed, access to their personal data, and the following information:

- the purposes of the processing
- the categories of personal data concerned
- the recipients or categories of recipient to whom the personal data have been or will be disclosed
- how long the data will be stored or the criteria used to determine the retention period
- the right to request rectification or erasure of personal data, restriction of processing or object to processing
- the right to make a complaint.

2.2.1 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request about their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at LifeLine School may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

2.2.2 Subject access procedures

- a) Any request to access personal data can be made verbally, or in writing to the relevant manager.
- b) The manager will acknowledge the request in writing.
- c) The manager will prepare the personal data for viewing.
- d) Where relevant, all third parties are written to, stating that a request for disclosure has been received. Permission will be sought to disclose the data to the person requesting it. Copies of these letters are retained on file. Third parties include:
 - family members
 - workers from agencies, including social services and health authorities etc. It is usual for agencies to refuse consent to disclose, preferring the individual to go directly to them.
- e) Copies of these letters and their replies are kept on file.
- f) A photocopy of the complete file is taken.
- g) The manager redacts any information which a third party has refused consent to disclose. This is done with a redacting marker and every reference to the third party and information they have added to the file is removed.
- h) What remains is the information recorded by LifeLine and that of any third parties who have agreed to their information being disclosed. This is called the 'clean copy'.
- i) The 'clean copy' is photocopied and the individual requesting access is invited in to discuss the contents. Alternatively, the file can be sent by secure email.
- j) Legal advice may be sought before sharing a file, especially where there are possible grounds for litigation against LifeLine, or a third party.

2.3 Right to rectification

Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.

When we receive a request for rectification, we will take reasonable steps to satisfy ourselves that the data is accurate and to rectify the data if necessary. Where it applies, we will take into account the arguments and evidence provided by the data subject.

What steps are reasonable will depend on the nature of the personal data and what it is used for. The more important it is that the personal data is accurate, the greater the effort we will put into checking its accuracy and, if necessary, taking steps to rectify it. For example, we will make a greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones. We may also take into account any steps we have already taken to verify the accuracy of the data prior to the challenge by the data subject.

Whilst we are checking the accuracy of data, we will restrict processing activities until where have verified its accuracy.

Personal data is inaccurate if it is incorrect or misleading as to any matter of fact. We will update any data found to be inaccurate immediately and inform the individual we have done so.

2.3.1 Opinions

It can be difficult to conclude that an opinion is inaccurate. Where we record an opinion, our records will show clearly that information has been recorded as an opinion, and, where appropriate, whose opinion it is.

2.3.2 What we will do if we are satisfied the data is accurate

We will explain to the individual that we have checked their personal data, that we are satisfied it is accurate and that we will not be amending the data. We will also inform the individual of their right to complain.

2.3.4 Informing other organisations

Where we have disclosed personal data to others, we will contact recipients and inform them of the rectification or completion of the personal data.

2.4 Right to erasure (also known as the 'right to be forgotten')

Individual's have the right to have personal data erased in certain circumstances. These are:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for
- we are relying on consent as the lawful basis for holding the data, and the individual withdraws their consent
- we are relying on legitimate interests - see appendix E, Legitimate Interests Assessment, as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing
- we are processing the personal data for direct marketing purposes and the individual objects to that processing
- we have processed the personal data unlawfully
- we have to erase the data to comply with a legal obligation.

We will give particular weight to any request for erasure if the processing of the data is based upon consent given by a child, especially any personal data processed on the internet. We do not process personal data to offer information society services (online services) to children.

2.4.1 Who we tell about personal data that has been erased

We will tell other organisations about the erasure of personal data where:

- The personal data has been disclosed to others – we will contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort.
- The personal data has been made public in an online environment e.g. social networks, forums or websites – we will take steps to inform other controllers who are processing the personal data to erase links to, copies or replication of that data. In doing this, we will take into account available technology and the cost of implementation.

2.4.2 When does the right to erasure not apply?

The right to erasure does not apply if processing is necessary for one of the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation.
- For the performance of a task carried out in the public interest or in the exercise of official authority.
- For archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing.
- For the establishment, exercise or defence of legal claims.
- If special category data is necessary for public health purposes in the public interest or if the processing is necessary for the purposes of preventative or occupational medicine.

2.5 Right to restrict processing

Individuals have the right to restrict the processing of their personal data in certain circumstances.

This means that an individual can limit the way that LifeLine uses their data. This is an alternative to requesting the erasure of their data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information we hold or how we have processed their data. In most cases we will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.

2.5.1 When does the right to restrict processing apply?

Individuals have the right to request that LifeLine restricts the processing of their personal data in the following circumstances:

- The individual contests the accuracy of their personal data and we are verifying the accuracy of the data.
- If an individual has challenged the accuracy of their data and asked LifeLine to rectify it, they also have a right to request their data is restricted while we consider their rectification request.
- The data has been unlawfully processed and the individual opposes erasure and requests restriction instead.
- We no longer need the personal data but the individual needs LifeLine to keep it in order to establish, exercise or defend a legal claim.

- The individual has objected to LifeLine processing their data and we are considering whether our legitimate grounds override those of the individual.
- If an individual exercises their right to object, they also have a right to request that we restrict processing while we consider their objection request.

There are many ways in which data can be restricted and where we receive a request, we will use the most appropriate method, such as:

- making the data unavailable to users
- temporarily removing published data from a website.

We will ensure that restriction includes all forms of processing, including collection, dissemination and erasure of data.

We will consider how we store personal data that we no longer need to process but the individual has requested we restrict (effectively requesting that we do not erase the data). This will include, where appropriate, the use of technical measures to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. We will also note on our system that the processing of this data has been restricted.

2.5.2 What we do with restricted data

We will not process the restricted data in any way except to store it unless:

- we have the individual's consent
- it is for the establishment, exercise or defence of legal claims
- it is for the protection of the rights of another person (natural or legal)
- it is for reasons of important public interest.

2.5.3 Who we will tell about the restriction of personal data?

If we have disclosed the personal data in question to others, we will contact each recipient and inform them of the restriction of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, we will also inform the individual about these recipients.

2.5.4 When can we lift the restriction?

In many cases the restriction of processing will only be temporary, specifically when the restriction is on the grounds that:

- The individual has disputed the accuracy of the personal data and we are investigating this.
- The individual has objected to LifeLine processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of our legitimate interests, and we are considering whether our legitimate grounds override those of the individual.

Once we have made a decision on the accuracy of the data, or whether our legitimate grounds override those of the individual, we may decide to lift the restriction.

When we lift a restriction, we will inform the individual before we lift the restriction.

2.6 Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Data portability does not apply to LifeLine as we do not process personal data by automated means.

2.7 Right to object

The right to object effectively allows individuals to ask LifeLine to stop processing their personal data in certain circumstances.

The right only applies in certain circumstances and whether it applies depends on our purposes for processing and our lawful basis for processing.

2.7.1 Direct marketing

Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes. However, at the time of writing this policy, LifeLine does not undertake direct marketing activities.

2.7.2 Public task or legitimate interests

Individuals can also object if the processing is for:

- a task carried out in the public interest
- the exercise of official authority
- LifeLine's legitimate interests (or those of a third party).

In these circumstances the right to object is not absolute. At the time of writing this policy, LifeLine does not carry out tasks in the public interest or, for the purposes of exercising official authority.

In respect of legitimate interests, an individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their particular situation. In these circumstances this is not an absolute right, and we can continue processing if:

- we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- the processing is for the establishment, exercise or defence of legal claims.

We will explicitly bring the right to object to the individual's attention and will present this information clearly and separately from any other information.

2.7.3 Research purposes

Individuals can object if the processing is for scientific or historical research, or statistical purposes, in which case the right to object is more limited. However, at the time of writing this policy, LifeLine does not process data for scientific or historical research. We may process data for statistical purposes and, where this applies, we will ensure we have appropriate safeguards in place e.g. data minimisation and, where possible, pseudonymisation.

We will inform individuals about the right to object in our privacy notices.

2.7.4 Action we will take when we receive a right to object

We will stop processing the data if we receive an objection to the processing of personal data and we have no grounds to refuse.

We will review the data we hold and erase the data appropriate to the objection.

2.8 Rights related to automated decision making including profiling

This right does not apply as LifeLine does not make decisions about individuals using automated means and does not use automated processing of personal data to evaluate certain things about an individual.

3. How we respond to requests

Individuals can exercise their rights by making a request verbally or in writing.

3.1 Fees

In most cases we will not charge a fee to provide information requested.

However, where we consider a request is manifestly unfounded or excessive, we will charge a fee to cover the administrative costs of complying with the request.

We will also charge a fee if an individual requests further copies of their data following a request. Again, the fee will be based on the administrative costs of providing further copies.

Alternatively, we may refuse to respond to a request, for example, if we consider a request to be malicious or the request overlaps with other requests. Where this is the case, we will inform the individual, at the latest within one month of receipt of the request, the reasons we are not taking action. We will also advise the individual of their right to complain.

3.2 Timescales for responding to requests

We will act on requests without delay and at the latest within one month of receipt of the request. The time limit is calculated from the day after we receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

We may extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

3.3 Confirming identity

If we have doubts about the person making the request, we will ask the individual to confirm their identity before responding to their request. We will let the individual know this requirement as soon as possible. The period for responding to the request begins when we receive confirmation of identity.

4. Complaints

Individuals can make a complaint if they believe LifeLine has not processed their personal data in accordance with the GDPR and the Data Protection Act 2018.

Complaints will be investigated by the Quality Manager in accordance with the LifeLine complaints policy that is available on <http://www.LifeLineprojects.co.uk/policies/>

Alternatively, complaints can be made in writing to:

Director of Finance and Operations
LifeLine Community Projects
LifeLine House
Neville Road
Dagenham
Essex
RM8 3QS.

Individuals can report concerns to the Information Commissioner's Office (ICO) on 0303 123 1113 or online via the following link: <https://ico.org.uk/concerns/>

Part three - information security

LifeLine processes personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage. We have implemented appropriate technical and organisational measures e.g. cybersecurity (protection of networks and information systems from attack) and other measures such as physical security, to ensure levels of security appropriate to the risk.

LifeLine subcontracts the management of IT security and maintenance to One Stop Cloud Ltd TA Integrity who are also contracted to provide IT support services.

Records

We ensure records containing personal data are maintained in a safe and secure environment and that only authorised staff, as shown in the table below, can access, alter, disclosure or destroy personal data.

Type of data	Who has access
Beneficiary records	Authorised staff and managers
Budgets	SMT, finance staff and budget holders
Child protection records	DSL and deputy and DSO's
Finance and payroll records	Finance and HR staff
HR records	HR staff and managers
Management accounts	SMT
Organisational records i.e. leases, deeds, insurance, charity and company registration, health and safety	SMT and authorised support services staff and managers

We also ensure that staff only act within the scope of their authority.

Security measures include, but are not limited to, paper-based documents and electronic content such as email, word processed documents, spreadsheets, presentations, databases, CCTV images and photographs.

The following sections detail the measures in place to ensure the security of records, the physical security of buildings and cybersecurity.

3.1 Paper records

Paper records (e.g. confidential HR, business records and beneficiary records containing personal information) are stored in industry-standard lockable filing cabinets/cupboards. Lockable desk storage is provided to all staff.

Documents are stored/filed by contract or function. Responsibility for adequate storage is delegated to the relevant manager who must manage storage as detailed below:

- Filing cabinets must be placed in a secure environment that are not accessible to unauthorised personnel.
- Filing cabinets must be kept locked at all times and unlocked when information needs to be removed.
- The keys to filing cabinets must not be left in locks.
- Access by staff to confidential information is limited to 'a need to know' basis.
- Protectively marked paper documents must not be copied or electronically scanned without the consent of the contract manager or responsible director.

3.2 Electronic records

Staff are provided with IT hardware and software (e.g. desktop PCs, laptops, tablets and/or smartphones or other mobile devices) necessary to carry out their job role. Staff are also given access to the parts of the network needed to fulfil the job role.

Lifeline does not operate a 'bring your own device' to work system and staff are not permitted to use their own devices for business purposes.

Access to the network is controlled by user IDs and passwords. All IDs and passwords are uniquely assigned to named individuals who are accountable for all actions on their account.

To prevent unauthorised access to information, staff must not:

- Allow anyone else to use their user ID and/or password.
- Leave their user accounts logged in at an unattended/unlocked computer.
- Use another member of staffs' user ID and password to access the network.
- Leave their password unprotected (for example by writing it down).
- Perform any unauthorised changes to the network or information.
- Exceed the limits of their authorisation to interrogate the IT system or data.
- Connect any unauthorised (non-Lifeline) device to the network e.g. personal mobile phones.
- Store Lifeline data on any non-authorised equipment.
- Give, or transfer data or software to any person or organisation outside Lifeline without express authorisation to do so.
- Store work on the desktop, or in the documents folder on the 'S' drive.

Managers must identify whether there is an operational need for the use of portable storage to securely store personal or special category data and make arrangements to purchase suitable encrypted memory sticks, and provide staff with training in their use.

3.3 Clear desk and clear screen policy

3.3.1 Clear desk

A clear desk is a workspace that prevents unauthorised access to confidential information (e.g. commercial, personal or special category personal data).

To minimise the risk of unauthorised access or loss of information, staff must follow the clear desk policy:

- In-trays must not be used to store documents that contain personal or sensitive personal information.
- Encrypted memory sticks must not be left in devices when unattended.
- Desktop computers and laptops must be locked by pressing Ctrl-Alt-Delete when unattended.
- At the end of the work day, all IT applications must be closed down and the work station logged off and shutdown correctly.
- Laptops must be stored securely and not left out on desks at the end of the day, or when the user is not in the office.
- Minimise the amount of printed personal/special category information kept on desks.
- Personal or special category data must be stored in locked in filing cabinets when not in use.
- All document storage is to be kept locked when not in use (e.g. filing cabinets, desk drawers).

3.3.2 Clear screen policy

It is the responsibility of managers to inform staff where they can save their work on the 'S' drive. This will be in a folder on the 'S' drive that is only accessible to staff who need access to the information.

Staff are not permitted to store any files on their desktop (e.g. word and excel documents).

Staff who process confidential information should consider the use of privacy screens to minimise data being accessed inadvertently by unauthorised personnel.

3.4 Moving documents

There will be circumstances where personal information needs to be taken off site or, information gathered off-site needs to be taken to the office.

The risks from loss or theft can increase when transferring personal information by hand, or taking personal information off site for meetings. The following points should be considered and, if necessary, action taken to mitigate any identified risks proportional to the amount and sensitivity of the information being transferred:

- Consider if the information can be saved on an encrypted memory stick or laptop for transit rather than transferring in a printed format; if using this method, consider how the information will be printed/ downloaded/accessed on arrival.
- During the transfer, maintain the security of the information by using a lockable briefcase or similar.
- If using public transport keep the information with you at all times.
- If travelling by car, store the information in the boot of the car during transit.
- Consider how you can identify and label the material in some way so if lost/stolen and then subsequently found by a member of the public it can be identified as LifeLine property and safely returned. Printed material can be placed in a sealed envelope and labelled as 'Property of LifeLine, if found please return to....'
- The need to store personal data overnight at home should be avoided if possible. If this is unavoidable, personal information should be stored in a lockable container which is not accessible to other people.
- Staff must report any information loss immediately to their line manager.
- Staff are responsible for recording information loss on the serious incident log on SharePoint.

3.5 Use of email

The following applies to all staff who have a LifeLine email account:

- To ensure the security of LifeLine's network, staff must not open any email attachment in their inbox if they do not recognise the sender.
- Staff must not reply to unexpected emails requesting their security information details e.g. network log-in, password or answers to security questions. Legitimate emails will never ask for this information.
- Where an email is being sent to recipients who do not know each other, staff must use BCC (blind carbon copy). This means that email addresses are not shared between all the recipients without consent.
- Staff must delete non-essential e-mail messages on a regular basis. The email archive facility should be used to clear received and sent email boxes of correspondence that is no longer current but which needs to be retained for evidence and/or other purposes – see annex B, retention schedule for retention periods.
- Staff are not permitted to send business emails containing personal or special category data about beneficiaries, or commercially sensitive information, to personal email addresses unless there is a necessary business reason to do so.

- All outgoing LifeLine business e-mails have an automatic footer which contains a legal disclaimer. LifeLine staff are not permitted to amend or delete the footer. Integrity must be notified if the footer is not visible in an email template.
- Emails sent on behalf of another member of staff must be clearly marked as such on the email. Failure to do so may constitute fraud or mis-representation.
- The recommended out of office setting is:

“This is the mailbox of {add name}. Unfortunately, I am not available to respond to your message until (.....). If the matter is urgent please contact {add name and contact details}. If the matter is not urgent I will respond to your message as soon as possible. Thank you”.

3.5.1 Sending personal/special category data by email

Staff are not permitted to send personal or sensitive personal information unprotected by email to external recipients and must follow the rules below before emailing such information:

Increasing document content sensitivity			
LOW (unclassified)	MEDIUM (protected)	HIGH (restricted)	VERY HIGH (confidential)
Definitions			
No restriction	The only circumstances beneficiary details can be included in the body of an email is where the information provided cannot identify an individual e.g. D. Lewis or Daniel Lewis.	<p>The following rule is to be followed where it is planned to send only one record by email:</p> <p>Personal or special category information that can identify an individual must be protected before it is sent. The information must be recorded in a separate document that is password protected.</p> <p>The password to open the document must be communicated to the recipient by a different method e.g. telephone or via a separate email).</p> <p>The following rule is to be followed where it is planned to send more than 10 records:</p> <p>Staff are not permitted to send more than 10 records containing personal or sensitive personal information by email/attachment to email.</p> <p>Information must be either couriered or transferred onto an encrypted memory stick and posted by special delivery.</p>	

3.6 Use of telephone, fax, email and internet

This section covers the security and use of devices and services provided to staff to conduct business activities. All individuals are accountable for their actions when using devices and services.

3.6.1 Telephone (landline and mobile)

Staff must follow the guidelines below when using telephone equipment:

- Use of telephone equipment is intended for business use. Individuals must not use facilities for sending or receiving private communications on personal matters, except in exceptional circumstances.
- When working in public places staff must be mindful that they could be overheard and inadvertently share personal information. Staff should check they cannot be overheard before discussing personal information.
- Mobile phone users must ensure their device is protected through the use of a password or pattern lock.

- To minimise potential data loss, when storing beneficiary contact details only the name and phone number should be stored on a mobile device.
- Where possible, remote wipe facilities on mobile phones should be enabled to allow for all data to be securely wiped from the device in the event of loss or a theft.
- The loss of a mobile phone must be reported immediately to your line manager.
- The incident must also be reported using the incident reporting button on SharePoint.

3.6.2 Telephone voicemail

- The recommended voicemail message is:

'You have reached the voicemail of {add name}. Unfortunately, I am not available to take your call at the moment/until. Please leave a brief message, with your name and telephone number and I will return your call as soon as possible. Alternatively, contact {add name and contact details}. Thank you'.

- Where applicable, it is recommended that voicemail passwords are changed at the same time as changing PC passwords.

3.6.3 Text/messaging services

When a beneficiary contacts a member of staff by text message, the staff should not reply to the text but contact the beneficiary by phone to verify the caller's identity. This minimises the risk of unauthorised data disclosure.

3.6.4 Fax

A fax uses a telephone line to complete a point to point transfer of information. This is more secure than an email or the use of internet that uses an open system that can be intercepted. Guidelines for sending faxes are shown below:

- All outgoing faxes must be accompanied by a LifeLine fax header sheet that records the number the fax is being sent to and lets the recipient(s) know who the information is for and whether it is confidential or sensitive.
- When sending personal or special category information by fax, ask the recipient to confirm that they are at the fax machine, ready to receive the document and that there is sufficient paper in the machine. Telephone or email to make sure the whole document has been received safely.
- When receiving faxes, reduce the risk of accidental disclosure or data loss by making sure that faxes are collected immediately so that confidential information is not left unattended.
- Built-in message stores, page caches and incoming fax stores must be cleared regularly by staff nominated to carry out this function.

3.6.5 Internet

Use of LifeLine internet and email is intended for business use.

Personal use is permitted where:

- such use does not affect the individual's business performance or contracted working hours
- use is not detrimental to LifeLine in any way, not in breach of any term and condition of employment and does not place the individual, or LifeLine, in breach of statutory or other legal obligations.

3.6 Post

Staff who dispatch post must follow the instructions below to ensure that information is sufficiently protected based on its content, sensitivity or the amount of information being posted.

3.6.1 Outgoing post

Protective Markings				
Increasing document content sensitivity				
Low (unclassified)	Medium (protected)	High (restricted)		Very high (confidential)
Definitions				
A public domain document containing no personal information	A document that contains personal information but does not allow for individuals to be identified	Personal data that enables a living individual to be identified from a group e.g. <ul style="list-style-type: none"> • name • address • medical details or banking details 		Information that contains sensitive personal data e.g. personal data plus one or more of the following sensitive data: <ul style="list-style-type: none"> • ethnic background • political opinions • religious beliefs • health • sexual health • criminal records
Can be sent by post	Can be sent by post	Can be sent by post if letter only contains information about one person.	Must be sent by special delivery if letter contains information about two or more people.	Must be sent by special delivery or by courier

3.6.2 Incoming post

Incoming post, special deliveries, couriers or parcels are processed as follows:

- All post sent generically to LifeLine is opened and forwarded to the relevant department.
- Post for the finance department (e.g. cheques, invoices etc.) are always sent to the Finance department irrespective of the address on the envelope.
- Incoming letters marked with a security classification or addressed to a named person are delivered directly to the addressee.
- Post received via courier will be signed for by staff receiving the delivery. Recipients will be notified about the delivery and arrangements made for collection.

3.7 Physical security

3.7.1 Building access control

A named manager will have responsibility for maintaining building security at all times. Security is managed as follows:

- Staff can only access LifeLine premises during normal business hours; these may vary in each location based on the nature of the service delivered. Approval must be gained from a director if a member of staff requires access outside of usual office opening hours.
- Entrances and exit points at some premises are covered by CCTV.
- Doors leading to the private areas in a building must not be left unbolted, unlocked or propped open.

3.7.2 Dealing with visitors

- All visitors must sign in and out of LifeLine House.
- Visitors who cannot verify their identify will not be granted access.

- All visitors who need access to secure areas in a building must be accompanied.

3.7.3 Rooms with secure access

The following will apply to buildings that have secure access rooms e.g. server rooms and electrical cupboards:

- Access to secure areas, including those where personal or sensitive personal information is processed (including conversation), is restricted to authorised staff.
- A member of SMT, or a named delegated individual, is responsible for authorising access to secure areas.
- Each secure area will have an assigned owner with a contingency for absence.
- A secure area owner is responsible for ensuring that security controls are maintained.
- Secure areas must be locked at all times.
- Authorised persons are issued with relevant access codes or keys.
- The member of staff responsible for a secure area is responsible for ensuring that no unauthorised activity takes place within the area.
- Access required by a service contractor to work in a secure area must be logged by the member of staff responsible for that area. This could be in the form of an email confirmation from the contracting organisation stating what needs to be done, when they will be on site and who will be attending. The consultant or contractor will sign in and out of the building at reception.

3.7.4 Locking/unlocking

Each LifeLine site has a list of staff authorised to lock and unlock a building.

This is in addition to key holders who are staff that have sets of keys but who do not normally open or close buildings.

Opening and closing procedures at each site is based on the requirements of the building and will therefore be different. The procedures below are to be followed for locking and unlocking buildings:

- Staff cannot be authorised to lock or unlock a site until their competence has been signed off by an appropriate manager.
- Staff are not permitted to disclose their codes (e.g. padlock or alarm codes).
- Additional care needs to be taken where a member of staff locks or unlocks a building alone. Once the intruder alarm is de-activated, the lone member of staff must lock the door to the building until additional staff arrive.
- Under no circumstances is a lone member of staff to accept a delivery, open a door to a beneficiary, or place themselves in a situation that may place them at risk of being attacked, or coerced into allowing unauthorised access.
- If a key holder is called to attend a site out of hours due to alarm activation, care needs to be taken to ensure the alarm activation has not been caused by individuals lying in wait for the key holder to attend so they can gain unauthorised access.

A lone female employee responding to an alarm activation can request local police attendance before entering the site.

3.7.5 Closed circuit television (CCTV)

LifeLine is a system operator for CCTV which is used as a tool to protect people and property. It also provides protection for staff, children and visitors to our premises where clarification is needed on any incidents or accidents that may arise.

Our CCTV systems are used to record the activities of identifiable individuals. These images are treated as personal data under the General Data Protection Act (GDPR) and the Data Protection Act 2018 (DPA).

Lifeline does not use audio recording, facial or other biometric characteristic recognition systems or covert surveillance. Our CCTV system users do not require a SIA licence. We do not intend to record or capture information that is intrusive.

Lifeline has adopted the 12 Guiding Principles that form part of the Surveillance Camera Code of Practice published by the Home Office. We have used the guiding principles to establish a clear rationale for the use of overt CCTV, to help us run our systems effectively, help ensure compliance with other legal duties and to maximise the likelihood of achieving surveillance by consent.

No	Guiding Principle	Lifeline arrangements to ensure compliance with principles
Principles 1 to 4: the development or use of surveillance camera systems		
1	Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need	Lifeline will only use CCTV for the purposes it was installed. It will not be used for other purposes that would not have justified its needs in the first place.
2	The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified	The effects of the use of CCTV on individuals and their privacy will be assessed through the use of a data privacy impact assessment screening tool. The use of CCTV will be reviewed periodically to ensure its use remains justified.
3	There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints	Signage makes staff and the public aware that they are being monitored by a CCTV system that is operated by Lifeline and the purpose for which CCTV is used e.g. to protect property. The signage also includes a contact email address where individuals can obtain further information.
4	There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used	Each location has a named system owner who is responsible and accountable for the data processed by CCTV systems.
Principles 5 to 12: the use or processing of images or other information obtained by virtue of such systems		
5	Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them	Lifeline will ensure that staff who have responsibilities within the management or operation of CCTV systems are competent, have relevant knowledge, skills and training on the operational, technical and privacy considerations of the system and fully understand policies and procedures relating to CCTV. New staff will be informed about the use of CCTV as part of staff induction and through the use of signage. We will manage CCTV within a robust operating environment that demonstrates to the public and staff that the system is operated responsibly, effectively and the likelihood of any breach of individual privacy is greatly reduced.
6	No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged	Images and information will not be kept for longer than necessary to fulfil the purpose for which they were obtained in the first place. Retention periods for CCTV images are stated in Lifeline's Information Retention Schedule - see appendix B.
7	Access to retained images and information should be restricted and there must be clearly	Access to retained images and information will be restricted to the relevant system owner and system users attached to that system owner. Other staff may

	defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes	be authorised to access retained images for specific purposes e.g. internal auditors. Disclosure of information from CCTV is controlled and is consistent with the purpose(s) for which the system was established. For example, because we have installed CCTV to protect people and property, it is appropriate to disclose surveillance information to the Police to prevent and detect crime. LifeLine will not publish CCTV footage on the internet.
8	Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards	Due to the small number of CCTVs cameras in operation, LifeLine does not currently consider it necessary to achieve external certification against operational, technical and competency standards.
9	Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use	Access to the recorded images is restricted to system owners and to a minimum number of system users. If images are specifically retained for evidential purposes i.e. following a break-in, the recording media will be retained in a secure place to which access is controlled by the system owner.
10	There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published	LifeLine is responsible for reviewing the continued use of CCTV to ensure the use remains necessary, proportionate and effective in meeting its stated purpose. Where appropriate, we will use the Surveillance Camera Commissioner's self-assessment tool as a guide to determine on-going compliance with the 12 Guiding Principles. The link to the tool is: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/372082/Self_assessment_tool_v3_WEB.pdf Reviews will include legal requirements, policies and standards. Any alternative methods of monitoring that carry less risk of invading individual privacy will also be considered. Any risks identified as a result of the review will be reported to the Director of Finance and Operations.
11	When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value	LifeLine ensures CCTV systems: <ul style="list-style-type: none"> • produce images and information of a suitable quality for use by the criminal justice system without enhancement • engage with relevant stakeholders to ensure exported data meets the quality required for it to be used of evidential purposes • ensure safeguards are in place to ensure the forensic integrity of images and information, including an audit trail • store information in a format that is easily exportable • ensure storage meets the integrity and quality of original recording and meta data.
12	Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date	This guiding principle does not apply to LifeLine.

3.8 IT security

LifeLine subcontracts the management of IT security and maintenance to One Stop Cloud Ltd, TA Integrity, who are also contracted to provide IT support services.

3.8.1 Physical security of IT equipment

The following measures are in place to protect equipment and information from theft and damage:

- LifeLine IT equipment is marked with an asset label.
- Physical access to network connection (wall sockets), scanning and fax facilities and networked printer points, are controlled by port access.
- Staff are not permitted to leave portable devices unattended in a public location.
- A full inventory log of IT equipment, including hardware and software, is maintained to keep accurate details of LifeLine devices.
- Equipment that is not used regularly is stored securely.
- Staff must report risks to security e.g. lost keys, missing locks to their line manager.
- Servers are sited in secure areas and access is limited to authorised staff.
- Staff are not permitted to move IT hardware and/or equipment (apart from portable devices) from its sited location without prior approval from their line manager.

3.8.2 Network security

To reduce the threat from Trojan software, LifeLine network users are not permitted to download and install any software from the internet.

Security software such as firewalls, virus checking, anti-malware and anti spyware is regularly updated to ensure it provides adequate protection. The network is segmented across a number of servers for practical and security reasons.

Detection, prevention and recovery controls to protect against malicious code are in place to protect the network from malicious attack. Network users have a responsibility to inform One Stop Cloud Ltd TA Integrity if they have a suspicion of being attacked by a virus, malware or spyware.

SMT will determine whether network penetration testing and social engineering is required. This will be performed by a suitably qualified organisation.

IT continuity planning is reviewed as part of the IT planning services provided by One Stop Cloud Ltd TA Integrity.

3.8.3 Email filters

The LifeLine network virtual email server is protected by a spam filter system provided by Force Point. The system is based online and monitors all incoming mail before it is downloaded to the LifeLine email servers. As a result, all spam and viruses are screened out at internet level and are not downloaded to the network. This ensures the infrastructure is free from disruption and congestion.

3.8.4 Device hardening

Local devices added to the network have a standardised build.

Access to operating systems is controlled by a secure administrative log-on procedure.

Local administrative rights are removed from local machines. This action prevents users from downloading and using, non-authorised, unlicensed software that can hide malware or malicious code on network devices.

Out-of-date or non-supported software is removed to reduce security vulnerabilities.

Default passwords on hardware and software are changed to reduce the vulnerability of an external attack.

3.9 Access controls

3.9.1 Network log-in

The table below details access rights by user classification:

Classification	Access Rights	Example
Non-network user	Can only use a stand-alone PC that is not connected to the network	
Temp Account	<ul style="list-style-type: none"> Limited access to folders on the shared ('S') drive based on the requirements of job roles Access to a temporary email account Access to SharePoint as a named user No 'U' drive. 	Temporary staff
Named Account	<ul style="list-style-type: none"> Default access to the 'S' drive based on requirements of job role Access to an email account Access to SharePoint as a named user. 	Full and part-time staff, office based volunteers
Remote Access (Named Account)	<ul style="list-style-type: none"> Default access to the 'S' drive based on requirements of job role Access to an email account Access to SharePoint as a named user. 	Required when a member of staff is frequently out of the office but who still requires access to the network, server and email
Administrator	Full unrestricted rights to: <ul style="list-style-type: none"> create folders on the main drives add users create user groups change settings manage the network. 	One Stop Cloud Ltd TA Integrity employees
Superuser	Full unrestricted rights to: <ul style="list-style-type: none"> all documents defined systems Can create and remove system administrators.	<ul style="list-style-type: none"> One Stop Cloud Ltd TA Integrity CEO.

3.9.2 Log-in/passwords

Access to the network is restricted to authorised user accounts as laid out in the table above. The following provisions apply to all network users:

- Network account holders are not permitted to use an account which is not their own.
- Network account holders are not permitted to disclose their password as this will allow unauthorised access to the system.
- The standard for password complexity is a minimum of 8 characters, including an upper and lowercase letter, a number and a special character (e.g. #, &, *, \$, £, !).
- Network users are prompted to reset their password every 90 days.
- An unused/idle device will automatically lock after a predetermined period of time.
- The network log-in is protected by a maximum of three log-in attempts before a password is disabled.
- When a member of staff leaves the employ of LifeLine, the relevant line manager will inform HR so that arrangements for managing the staff's email account can be agreed. For example, email accounts can be closed or access allowed to nominated staff so that incoming emails can be tracked or reassigned etc. This also applies to documents on 'U' drives. Integrity action changes to email accounts.

- Managers are responsible for checking that passwords are changed/disabled immediately when staff leave to prevent unauthorised access.
- When a staff member leaves, access to third party systems and databases will be disabled by the superuser for that system.

3.9.3 Wi-Fi

Wireless access to the network is provided by a secure Wi-Fi system (WPA 2-PSK) that is password protected. The password is changed every 90 days.

3.9.4 Guest access to the server

If a business need arises for a person who is not an employee of LifeLine to have access to the network, e.g. an external auditor or other guest, a temporary log-in to the network may be provided under the following circumstances:

- a member of SMT must approve the use of a temporary log-in
- server access will be restricted by folder access
- HR is responsible for requesting the deactivation of guest log-in accounts.

3.9.5 Remote access to the server

A remote access account may be required for employees who work away from a LifeLine site and who need to retain access to the network and the server. A request for a remote access account must be made to a line manager. Once approved, the request must be forwarded to tickets@integrity.help as a ticket request.

Employees with a remote access account working off site must ensure that any network connection via Wi-Fi is secure i.e. staff are not permitted to use an open/unsecured Wi-Fi service.

3.9.6 Network monitoring

LifeLine retains the right to monitor and log the activity of network user accounts. The purpose is to check for unusual activity, inappropriate or illegal behaviour.

Account monitoring and user activity logs form part of the measures taken to ensure the network is secure.

Information security logs/events are produced and kept for an agreed period to assist in future investigations and to support access control monitoring.

3.10 SharePoint

SharePoint is a web based application offering a set of tools that is used to provide an intranet portal within Office 365. It is not an encrypted system. SharePoint has a number of standardised uses that can be accessed by all staff, including:

- incident/accident or near miss reporting
- booking annual leave
- booking meeting rooms, equipment and reporting maintenance requests
- completion of sickness return to work forms
- document library for operational paperwork masters across programmes and contracts
- policies and procedures.

Access to SharePoint is restricted to users who have a network log-in.

A secondary layer of protection also restricts access to information within the SharePoint pages, files or folders. Access permissions are set for individual users or to a group of named users. Pages are organised by department, programme or function.

Staff are not permitted to store personal or special category personal data on SharePoint.

3.11 Third party applications/databases externally hosted

Contracts delivered by LifeLine may require staff to access and use externally hosted and managed MI systems. To reduce the risk of data being intercepted, copied or stolen, LifeLine staff using a third party application must do so only on a secure internet connection. An open/unprotected Wi-Fi connection must not be used to upload personal or sensitive personal data collected by LifeLine.

3.12 Back-up

To protect the integrity of the data on the network all servers are backed up by Integrity to a Datto appliance using varying schedules dependant on the role of the server. The last backup of each day is then transferred to the Datto Cloud and retained on a Grandfather, Father, Son retention policy.

In a catastrophic event all the servers can be started in a virtual environment on the Datto appliance and connected to the network as if they were the original server. If the building is lost, then the same recovery process can be run in the Datto Cloud and remote connectivity provided to Lifeline staff.

Data stored on Sage Line 50 is backed up to the 'F' drive daily.

3.13 Destruction and disposal of personal data

Personal data will be destroyed and disposed in line with the destruction dates stated in the Information Retention Schedule - see appendix B.

Personal data that has been archived off site will be securely destroyed at the offsite archive facility. Destruction receipts will be obtained.

3.13.1 Data Held Electronically

Information that has been archived electronically (e.g. on LifeLine's network) will be deleted securely.

Information archived on any other device such as hard drives, CDs, magnetic storage, portable storage, back-up devices, will undergo a process which will make the stored information irretrievable.

3.13.2 IT Asset Disposal

LifeLine's asset disposal process is based on the following waste hierarchy:

Prevention: in-house	<ul style="list-style-type: none"> Only order what is needed. Our internal controls (finance and equipment ordering processes) ensure equipment is only ordered when there is a business need. Reuse products in-house e.g. when staff leave LifeLine's employ equipment, is re-assigned to other staff. Obsolete equipment is returned to the relevant line manager who will arrange for it to be destroyed.
Prevention: external	<ul style="list-style-type: none"> Redundant ICT assets are sent to an external specialist IT asset disposal company to prepare for reuse (refurbishment and resale) or destruction. Leased equipment (e.g. photocopiers) are returned to the owner.
Recycling	<ul style="list-style-type: none"> Specialist IT asset disposal company will recycle any goods which cannot be reused.

3.13.3 Asset Disposal Process

Reusing devices in house:

- Devices are returned to Integrity, where they are reconfigured for use. This includes erasing all readily accessible personal data e.g. in the recycle bin.
- If devices can no longer be reused in house they are sent to a specialist IT asset disposal company for reuse, recycling or disposal.

The table below lists devices that may contain personal data and how it is wiped when the device is no longer required:

Device type	How personal data is wiped
Backup storage	Storage tapes are made daily. Tapes used are overwritten. Data tapes can be shredded by the specialist asset disposal firm.
CCTV images	By a specialist asset disposal firm.
Faxes	By a specialist asset disposal firm.
Laptop	By a specialist asset disposal firm.
PC	By a specialist asset disposal firm.
Photocopiers	Personal data must be wiped before devices are resold or recycled. Specialist advice on how to do this will be sought where required.
Printers	By a specialist asset disposal firm.
Servers	By a specialist asset disposal firm.
Smartphones and mobile phones	Are passed to Integrity who wipe all personal data off the phone. The phone is then re-issued or disposed of.
Tablets	By a specialist asset disposal firm.
USB	By a specialist asset disposal firm.

3.13.4 Process to Dispose of ICT Assets

Item	Actions required
1.	Complete an inventory of all equipment marked for disposal.
2.	Email the inventory to the waste disposal company before collection and to the Office Co-ordinator.
3.	On collection, and as each item of equipment is loaded, each item is checked off the inventory.
4.	The driver will ask for a Duty of Care (controlled waste) notice to be signed. A copy of the notice must be retained and given to the Office Co-ordinator. The other copy will be retained by the driver.
5.	<ul style="list-style-type: none"> • The asset disposal company will identify media that contains data. • The data is wiped from the media or physically destroyed. • A Certificate of Destruction is issued by the disposal company.
6.	The Certificate of Destruction is scanned and filed in the relevant folder on the 'S' drive.

Part four – management of personal data breaches

A personal data breach means a breach, accidental or deliberate, of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4.1 Personal data breach management

The management of the data breach will include the following:

- 4.1.1 All data security breaches, regardless of whether or not they need to be reported to the ICO, must be recorded using the Incident Log on SharePoint. The log gathers information about the facts of the breach, its effect and remedial action taken and gives an overview across the organisation about data security and the issues.
- 4.1.2 Containment and recovery – the response to the breach will include steps to recover personal data and where necessary, actions to be taken for damage limitation.
- 4.1.3 A risk assessment that identifies any risks associated with the breach and identifies the next steps to be taken. In particular, the risk assessment will assess the potential adverse consequences for individuals e.g. how serious or substantial these are and how likely they are to happen.
- 4.1.4 Informing individuals whose data has been breached, where applicable.
- 4.1.5 Investigation into the causes of the breach, and evaluation of the effectiveness of the actions taken to ensure it does not happen again. Policies and procedures will be updated if evaluation identifies the need.

4.2 Notification to the ICO

When a personal data breach has occurred, we will establish the likelihood and severity of the resulting risk to people's rights and freedoms. This is defined by the GDPR as "result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

If it's likely that there will be a risk to people's rights and freedoms, then we will notify the ICO by following the steps detailed in 4.3 below.

Breaches unlikely to be a risk will not be reported. The reasons for not reporting to the ICO will be recorded on the Incident Log on SharePoint.

Staff are not permitted to report breaches directly to the ICO without discussion with the Quality Manager who will seek authorisation from the Director of Finance and Operations.

4.3 How to notify the ICO

The ICO's data breach reporting form - see appendix F, must be completed before contacting the ICO to report a breach. The completion of the reporting form will ensure that we are prepared and can provide the information the ICO requires.

There are two ways to report a notifiable breach:

- 4.3.1 Call the ICO helpline on 0303 123 1113. Their opening hours are Monday to Friday between 9am and 5pm. The ICO will record the breach and give advice about what to do next, including how to contain it and how to stop it happening again. They also offer advice about whether we need to tell the data subjects involved.
- 4.3.2 Breaches can also be reported online - <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>. We can report online where we are confident that we have dealt with the breach appropriately or if we are still investigating and will be able to provide more information at a later date. The online form can also be used to report breaches outside the ICO's normal opening hours.

4.4 Timescale for reporting notifiable breaches to the ICO

Notifiable breaches must be reported to the ICO without undue delay, but not later than 72 hours after becoming aware of the breach. If it is not possible to report the breach within 72 hours we will contact the ICO and explain the reasons why.

4.5 Data processors

Our contracts with data processors who process data on behalf of LifeLine, for example Creative English hubs, include a clause that requires them to inform LifeLine, without undue delay, as soon as they become aware of a data breach. This requirement allows us to take steps to address the breach and meet our breach-reporting obligations.

Where LifeLine acts as a data processor e.g. has a contract that includes processing personal data, we will inform the contract holder, without undue delay as soon as we become aware of a data breach.

4.6 Telling individuals (data subjects) about a breach

If a breach is likely to result in a high risk to the rights and freedoms of individuals, we must inform those concerned directly and without undue delay. This may mean informing individuals before notifying the ICO i.e. this should take place as soon as possible. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach. We will follow the ICO guidance about what information to provide.

Part five - Responsibilities

An overview of board, committee and individual job holder responsibilities are shown below.

5.1 Board of trustees

Trustees have a duty of compliance, prudence and care (Charity Commission, March 2012). As such, their responsibilities include compliance with the requirements of other legislation and other regulators including the Information Commissioner's Office (ICO) who is the supervisory authority for data protection.

5.2 Senior management team

The Senior Management Team is responsible for:

- ensuring data protection risks are identified, assessed and treated
- ensuring data security breaches are investigated, recorded and reported, including where applicable, to the ICO and Charity Commission
- approval of the Data Protection policy
- undertaking annual data protection training.

5.3 Chief executive officer

The Chief Executive has overall responsibility for:

- ensuring LifeLine complies with the general law including the General Data Protection Regulation and the Data Protection Act 2018
- ensuring there are suitable and sufficient policies for IT Security and that they are kept up to date
- ensuring systems are in place to help prevent the loss/theft of personal data.

5.4 Directors

Are responsible for:

- ensuring DPIAs are completed where required
- ensuring all systems, services (including third-party services) and equipment used for storing personal and sensitive personal data meet acceptable IT security standards within their area of responsibility
- ensuring systems for IT maintenance are in place, including regular checks and scans to ensure security hardware and software is functioning properly
- checking and approving contracts with/for data processors.

5.5 Data Protection Officer

- reviewing and updating data protection policies, and related procedures, and submitting to SMT for approval
- answering data protection questions and providing general advice
- ensuring subject access requests are responded to within one month of the request being made
- preparing and submitting to SMT reports about potential and actual information security breaches, trends and incidents
- reporting actual or potential data breaches to the Director of Finance and Operations for further investigation
- ensuring reportable breaches are made in line with ICO timescales and requirements.

5.6 Human resources assistant

Is responsible for:

- conducting pre-employment checks and verifying the identity of new staff
- maintaining staff training and development records and monitoring completion of induction and information security training.

5.7 Managers

Are responsible for ensuring that they and their staff teams:

- understand the requirements of information security
- understand and implement contract requirements in relation to data protection
- are appropriately trained in the handling of personal and sensitive personal data
- complete annual information security refresher training
- keep paper files and other records or documents containing personal and/or sensitive personal data in a secure environment
- use secure passwords to protect personal data held electronically
- archive information, including paper and electronic records, for contracts and services that fall under their area of responsibility
- report actual or potential data loss to the relevant Director immediately and record the actual/potential loss on the incident log on SharePoint.

5.8 Communications manager

Is responsible for:

- addressing any data protection queries from journalists or media outlets
- ensuring marketing initiatives comply with data protection principles
- ensuring LifeLine complies with the requirements of the Privacy and Communication Regulations.

5.9 All staff

All staff have a responsibility to:

- protect the personal and special category data held by LifeLine
- take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss, disclosure or destruction
- ensure personal or special category data is not disclosed outside the requirements of this policy
- inform Integrity if they have a suspicion of being attacked by a virus, malware or spyware
- access or use personal data held about others for their own purposes
- report actual or potential data loss on the serious incident log on SharePoint.

6. Specialist and competent person advice

LifeLine used GDPR assessment tool and other resources on the ICOs website to develop this policy.

7. Implementation and monitoring

7.1 Implementation

Once approved, this policy will be available on SharePoint and the previous versions of the policy and associated documents removed. LifeLine maintains an electronic archive of all policy documents.

7.2 Process for monitoring implementation and effectiveness

For this policy, the following monitoring processes are in place.

Standard	Monitoring process
Conduct data protection privacy impact assessments (DPIAs), where relevant, at contract implementation stage	Documented in implementation plan and DPIAs.
Deliver information security awareness raising to all staff	Confirmation from staff that they have read, understood and will comply with requirements. Central training records maintained by HR who will provide reports on levels of completion.

Spot check audits to measure compliance	Documented in audit reports.
Review data security incident log	All incidents (potential/actual breaches) reported periodically to SMT.

8. References

Action Fraud: <http://www.actionfraud.police.uk/>

Auditing Data Protection: A Guide to ICO Data Protection Audits

https://ico.org.uk/for_organisations/data_protection/working_with_the_ico/~media/documents/library/Data_Protection/Detailed_specialist_guides/auditing_data_protection.pdf

Computer Misuse Act 1990 <http://www.legislation.gov.uk/ukpga/1990/18/contents>

Data Protection Act 2018 <http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

Guide to General Data Protection Regulation <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>

Information Sharing July 2018: Advice for practitioners providing safeguarding services to children, young people, parents and carers

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721581/Information_sharing_advice_practitioners_safeguarding_services.pdf

Privacy and Electronic Communications Regulations <http://www.legislation.gov.uk/uksi/2003/2426/contents/made>

9. Related documents


This policy must be read in conjunction with the policies regarding the safety and welfare of children. These together make up the suite of policies to safeguard and promote the welfare of children:

LifeLine Institute	e-Safety
Little Learners	CCTV
	Complaints
	Data protection
	e-Safety
	Staff code of conduct
Other related LifeLine policies	Use of mobile phones and cameras
	Complaints
	Risk management strategy
	Safeguarding and child protection

10. Definitions

The following are a list and description of the meaning of key terms used in this policy.

Term	Description of Term
Anti-virus	Is protective software designed to defend computers against malicious software.
Anti-malware	Is a type of software program designed to prevent, detect and remove malicious programming on individual computing devices and IT systems.
Data controller	An organisation who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other staff.
Data Protection Officer	Nominated member of staff who assists with monitoring internal compliance, informs and advises on data protection obligations, provide advices regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the ICO.
Data processor	An organisation who processes personal information on a data controller's behalf, for example outsourcing the disposal of confidential waste to an external company.

Data sharing	The disclosure of data from one or more organisations to a third party organisation, or the sharing of data between different parts of an organisation.	
Data subject	The identified or identifiable individual whose personal data is held or processed.	
ICO	Information Commissioner's Office, the UK's independent body set up to uphold information rights.	
Incident log on SharePoint		LifeLine's incident log, accessible to all staff, that is used to record any serious incident, including data breach/loss, damage/loss of equipment and near misses. The log is located on the front page of SharePoint.
Data Protection Impact Assessment (DPIA)	A process that determines data protection risks in the collection of personal and special category personal data and arrangements for mitigating identified risks.	
Integrity	Third party IT service provider.	
Privacy Notice	A statement that explains to individuals how LifeLine processes their data.	
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: <ul style="list-style-type: none"> • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.	
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.	
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.	
Recipient	A natural or legal person, public authority, agency or other body to which the personal data is disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.	
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation 	
Spam filter	Software which checks incoming email for malicious content or unsolicited email.	
Subject access request (SAR)	A subject access request (SAR) is a verbal or written request made by or on behalf of an individual for the information which he or she is entitled to ask for under 'Right of Access' of the GDPR.	

11. Version control

Version	Date	Author(s)	Status	Comment
6	Nov 2012	Dave Gibbons	Approved	
7	Dec 2015	Julia Ward Dave Gibbons	Approved	
8	Dec 2018	Julia Ward	Pending	Update with GDPR and DP 2018 regulations
9	16/01/20	Julia Ward	Approved	General update

Appendix A - ICO certificate of registration
Appendix B - Information retention schedule 2019
Appendix C - Data protection privacy impact screening template
Appendix D - Data protection impact assessment template
Appendix E - Legitimate interests' assessment template
Appendix F - ICO Report a personal data breach template