| Licensed Trade Charity: Organisation Policies and Procedures | | | |
|---|---|---|---|
| **IT POLICY** | | | |
| Effective Date: | 15th March 2019 | Title: Data Protection Policy | |
| Supersedes Date: | 8th March 2019 | | |
| | | Originator | Matt Smith / Adrian McGarry |

**Table of Contents**



## I PURPOSE

To provide adequate organisational policy and processes for Data Protection

## II RESPONSIBILITY

All line managers have a responsibility to uphold this policy and ensure their staff have read and are compliant with the policy, their responsibilities and the legal obligations surrounding the UK Data Protection Act 2018, EU General Data Protection Regulation, ePrivacy

## III SCOPE

This policy/procedure relates to the following areas:

| | | |
|---|---|---|
| **LTC** | **Yes** | ~~No~~ |
| **LVS** | **Yes** | ~~No~~ |
| **LVS Pupils** | ~~Yes~~ | **No** |
| **LVS Hassocks** | **Yes** | ~~No~~ |
| **Hassocks Pupils** | ~~Yes~~ | **No** |
| **LVS Oxford** | **Yes** | ~~No~~ |
| **Oxford Pupils** | ~~Yes~~ | **No** |

Exceptions to scope:

- None

## IV FREQUENCY

Organisation Policies and Procedures must be followed at all times.

## V GENERAL INFORMATION/DEFINITIONS

## Further information and updates can be found at:

- The https://ico.org.uk/ website
- Please click on the ICO links for help in understanding the General Data Protection Information and Data Protection Act
- Guidelines on data retention IRMS retention guidelines
- A guide to exemptions can be found on the ICO website here

## Definitions:

- *Personal data* means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
- *Sensitive Personal Data or Special Category Data* is personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Data relating to criminal offences and convictions are addressed separately (as criminal law lies outside the EU's legislative competence).
- *Pseudonymous data* Some sets of data can be amended in such a way that no individuals can be identified from those data (whether directly or indirectly) without a "key" that allows the data to be re-identified. A good example of pseudonymous data is coded data sets used in clinical trials
- *Data concerning health* means personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status. It expressly covers both physical and mental health.
- *Data Protection Principles* provide the conditions on which an organisation is permitted to process personal data. The principles are; Fair, lawful and transparent processing, the purpose limitation principle, data minimisation, accuracy, data retention periods, data security and accountability
- *DPO* Data Protection Officer

## VI POLICY

## Information rights

Good information handling provides a range of benefits as well as helping you to comply with the EU General Data Protection Regulation and Data Protection Act. The ICO has produced guidance for senior managers about taking a positive approach to information rights.

## *Data protection (looking after the information you hold)*

From the information that we hold within our organisation, we are legally obliged to protect that information; so under the EU General Data Protection Regulation, Data Protection Act, we must:

- ***Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject***
- ***Only collect information that you need for a specific, explicit and legitimate purpose***
- ***Ensure it is adequate, relevant, limited to what is necessary and up to date***
- ***Personal data must be accurate and, where necessary, kept up to date***

- ***Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed***
- ***Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures***
- ***We as the data controller are responsible for, and must be able to demonstrate, compliance with the Data Protection Principles***
- ***Allow the subject of the information to see it on request***

### *Our Legal Obligations*

### *Data usage*

#### Principle 1 of the GDPR states that data must be:

*"processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, transparency')"*

#### And Principle 2 of the GDPR states data must only be:

*"collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes"*

This means the data subject must be made aware of what data is being collected and how it will be used. This must be done in the form of a privacy notice. Once you have the data you must only process it in accordance with the privacy notice provided to the data subject. Processing data for a purpose other than the one(s) listed on the privacy notice is expressly forbidden unless you are legally compelled to do so.

This policy requires that you complete the eSafety modules and GDPR modules. These can be found on the LVSpace system.

https://senior.lvs.org.uk/course/view.php?id=479&section=2

For specific information on the handling of CCTV data please see the CCTV policy and code of practice

### *Security*

#### Principle 6 of the GDPR states that data must be:

*"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"*

#### File Storage

Any documents which contain personal data of any kind must be locked securely away and only taken out when being used.
Any documents that are no longer required should be disposed of securely. Shred them, do not simply bin them!

Remember that if something happens to the data because it was not securely stored, both your company and you could be found liable.
If in doubt, lock it away.

Documents that contain sensitive or special category data must be stored in our secure structured document repository, where these documents held can be managed, version controlled, indexed and audited.

## Encryption

To adhere to this GDPR principle all mobile and portable devices should be encrypted.
Be safe. Encrypt your data.

If you have an unencrypted USB stick or any other external storage device, then you have to encrypt this via Bitlocker from any of our network computers. Ask your line manager or the IT department for how to do this if you are unsure

Our email servers encrypt email automatically unless the recipient server does not understand encrypted emails when it will send the message unencrypted.

If you need to ensure that an email or documents are sent encrypted, then please refer to this training document here.

## Remote Wiping

Most modern mobile devices now come with a built-in remote data wiping function. This allows you or your IT department to wipe data from lost mobile devices.
Combine this functionality with an encrypted device and you are well on your way to adhering the “Integrity and confidentiality” principle of the GDPR.

Our email servers enforce this capability.
You need to inform the IT Helpdesk as soon as are aware that you have reported your device stolen or lost your device.
They can then (and only then) activate the remote wiping facility.

## Anonymisation & Pseudonymisation

Anonymisation and Pseudonymisation both have an important place in Principle 6. It is best practice to pseudonymise data sets which are currently in use, and to anonymise any data that is kept for statistical purposes or a purpose not specified in the Privacy Notice.
Pseudonymisation is the practice of splitting data to prevent identification. The data subjects can only be identified if both pieces (or possibly more) are put together. This is the best practice under GDPR and is highly recommended.
Anonymisation is different to pseudonymisation as the idea is to make the data subjects impossible to identify. It is most commonly used to keep data for statistical purposes. For example, a store would delete personal data such as address, names and payment details but keep data such as items purchased and date of purchase.

**Pseudonymise the data**
Current data should always, where possible, be pseudonymised to increase data security

**Anonymise the data**
Data repurposed for statistical use should always be anonymised

## Cloud Data

Data stored on external servers must meet GDPR requirements, no matter where the servers are located.

With this in mind make sure any services you use to comply with GDPR. Check their privacy and data protection policies as well as local laws if the servers are located outside of the EU.

Sensitive or special category data needs to housed onsite only. If something goes wrong the LTC will still be liable, even if you are using an external service to hold the data.

## Passwords

A good password policy is vital to help keep your data secure. Combining a strong password that is frequently changed with 2-factor authentication is ideal.
2-factor authentication is when you log in with a password and a code that is sent to you or generated for you at the time. Often the code is messaged to your phone or generated by a separate app installed on your mobile device.

**Minimum character limit:** A minimum character limit makes a huge difference; having more characters makes a password exponentially more difficult to brute force. A long password is one of the best ways to make your password more secure.

**Passwords must be changed frequently and old passwords cannot be reused:**
Changing passwords frequently and preventing the reuse of old passwords go hand in hand. It stops hackers with old/outdated information getting into your data.

**Use of nonsense/made up words:** There is no advantage to using nonsense or made up words as long as your password is of a sensible length.

**Must include numbers and special characters:** While many websites and companies will require numbers, capital letters and special characters in passwords these are not required. In fact, this is not best practice as it makes passwords harder to remember and as such reduces the length of passwords, thereby making them easier to brute force.

**Password Best Practice:**

- Use long password phrases instead of shorter random combinations Block the use of old passwords when users must change their password
- Frequent password changes
- Never tell anyone your password
- Do not write down usernames and passwords
- If possible, use 2-factor authentication

## Cyber Attacks

Cyber attacks are a major cause of data breaches. All staff have received elearning training, including social engineering techniques like phishing attacks, this is where criminals make contact by impersonating someone legitimate, they can then trick the person into giving them information or clicking a malicious link or file.
Remember; stay vigilant and use common sense.

## Audit Trails

Audit trails are extremely important for compliance with GDPR. Without well-defined and properly implemented workflow's an organisation cannot be compliant with the principle of “Integrity and Confidentiality” as they cannot ensure the integrity or confidentiality of the data they hold.

### *Data transfers*

Data can be transferred within the UK and within the EU as long as the user is aware of it (for example; it is mentioned in the Privacy Notice) and is aware why the transfer is taking place and we have a legitimate reason for making the transfer.

Any transfer to a non-EU country can only be made under the following conditions:

- made with the individual's informed consent;
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for the establishment, exercise or defence of legal claims;

If you wish to transfer data internationally and cannot meet one of the above conditions or you are unsure which applies, then you must contact your DPO before transferring the data.

### *People's rights*

If you receive a request regarding any of the following rights you must inform your DPO, this includes if you receive a request verbally.

#### The right to be informed

When collecting any data you must inform the person of what data you are collecting, why you are collecting it, how long you will keep it for, who has access to it etc. You can do this in the form of a Privacy Notice. You must contact your DPO to check or help you write the Privacy Notice.

#### The right of access & SAR requests

A Subject Access Request (or SAR) is an individual exercising their right to request information and copies of their personal data or the personal data of a child for which they have parental responsibility within our control and our systems.

It is your responsibility to inform the Data Protection Officer for your site of any requests pertaining to the EU General Data Protection Regulation or UK Data Protection Act 2018. The requests can make it explicitly clear that they are a SAR or may be in the form of somebody asking for all the data we hold on them, or a Freedom of Information Act request (even though we are not subject to the Freedom of Information Act).

To comply with these requests, we must respond within a one-month period, only with the information requested, concerning the individual.

No administration fee is applicable before processing unless the request is deemed by your Data Protection Officer (DPO) to be excessive or repetitive (if you believe a request to be excessive or repetitive then you must contact the DPO, but ultimately this assessment sits with the DPO).

All requests to process a SAR must be logged in the Data Protection Log, held in a secure area, under an encryption-protected file. Your DPO will log these requests.

Please be aware that any communications where an individual is identifiable will fall within a SAR and can, therefore be supplied to them.

Records processed by a teacher solely for the teacher's own use will be excluded from pupils' educational records.

## The right of rectification

Data subjects have the right to request that data held about them is rectified if it is found to be incorrect or misleading in anyway. This request may come in any form, for example; as an email, verbally or as a letter.

To comply with these requests, we must respond within a one-month period by correcting the inaccurate data and informing the subject that this has been done.

No administration fee is applicable before processing unless the request is deemed by your Data Protection Officer (DPO) to be excessive or repetitive (if you believe a request to be excessive or repetitive then you must contact the DPO, but ultimately this assessment sits with the DPO).

All requests to process a rectification request must be logged in the Data Protection Log, held in a secure area, under an encryption-protected file. Your DPO will log these requests.

## The right of erasure

Data subjects have the right to erasure, also known as the right to be forgotten. This can be received as a verbal or written request. However, this right is not absolute and does not apply in all circumstances. Always forward these requests to your DPO to deal with.

To comply with these requests, we must respond within a one-month period by either deleting the requested data and informing the subject or not deleting the data and informing them of the reason the data will not be deleted.

No administration fee is applicable before processing unless the request is deemed by your Data Protection Officer (DPO) to be excessive or repetitive (if you believe a request to be excessive or repetitive then you must contact the DPO, but ultimately this assessment sits with the DPO).

All right of erasure requests must be logged in the Data Protection Log, held in a secure area, under an encryption-protected file. Your DPO will log these requests.

## The right to restrict processing

Data subjects have the right to restrict processing, this means the users' data can be stored but not processed. This can be received as a verbal or written request. However this right is not absolute and does not apply in all circumstances. Always forward these requests to your DPO to deal with.

To comply with these requests, we must respond within a one-month period by either restricting processing and informing the subject or not complying and informing them of the reason the data will not be restricted.

No administration fee is applicable before processing unless the request is deemed by your Data Protection Officer (DPO) to be excessive or repetitive (if you believe a request to be

excessive or repetitive then you must contact the DPO, but ultimately this assessment sits with the DPO).

All right to restrict processing requests must be logged in the Data Protection Log, held in a secure area, under an encryption-protected file. Your DPO will log these requests.

If you wish to use data that has been restricted, you must first contact your DPO.

## The right to data portability

Data subjects have the right to data portability, this means subjects can request their data be sent to or shared with another organisation. This can be received as a verbal or written request. However, this right is not absolute and does not apply in all circumstances. Always forward these requests to your DPO to deal with.

To comply with these requests, we must respond within a one-month period by either providing the data in a common electronic format and informing the subject or complying and informing the subject of the reason for non compliance with the request.

No administration fee is applicable before processing unless the request is deemed by your Data Protection Officer (DPO) to be excessive or repetitive (if you believe a request to be excessive or repetitive then you must contact the DPO, but ultimately this assessment sits with the DPO).

All right to portability requests must be logged in the Data Protection Log, held in a secure area, under an encryption-protected file. Your DPO will log these requests.

## The right to object

Data subjects have the right to object to certain processing. This can be received as a verbal or written request. However, this right is not absolute and does not apply in all circumstances. Always forward these requests to your DPO to deal with.

To comply with these requests, we must respond within a one-month period by either stopping the processing of data as requested and informing the subject or not complying informing them of the reason we cannot comply with their request.

No administration fee is applicable before processing unless the request is deemed by your Data Protection Officer (DPO) to be excessive or repetitive (if you believe a request to be excessive or repetitive then you must contact the DPO, but ultimately this assessment sits with the DPO).

All right to object requests must be logged in the Data Protection Log, held in a secure area, under an encryption-protected file. Your DPO will log these requests.

***Your Data Protection Officers are:***

| | |
|---|---|
| ***LTC and Elvian Limited*** | ***Adrian McGarry*** |
| ***LVS Hassocks*** | ***Adrian McGarry, Matt Smith*** |
| ***LVS Ascot*** | ***Matt Smith*** |
| ***LVS Oxford*** | ***Austen Allen*** |

***Data Breach*** ..\Data Protection Breach Policy.doc

All staff are responsible for reporting data breaches to the DPO immediately on them becoming aware of any breach. This is the case even if you are not the member of staff that has caused the breach. Failure to do so will be subject to disciplinary action.

***Retention policy***

The retention and disposal periods connected to the general management of the organisation, follows IRMS retention guidelines, except where otherwise stated.

However, certain records will need to be retained indefinitely where they evidence permissions, provide standing data or to maintain an accurate financial, education or special educational needs picture over time.

***Retention assessment (Appendix A)***

## Data Retention Form

Process name: _____

Process owner: _____

What kind of data is captured for this process?
e.g Name, address, contact details etc.

| |
|---|
| |

Does the data have any specific laws regarding retention?
See appendix D of the Data Protection Policy for common legal retention periods

☐ Yes ☐ No ☐ Unsure

If yes:

State the data category: _____

State the legal retention period: _____

If yes skip to the end. If no continue the form.

How long will this data be in use?
Please try to justify the length of time

| |
|---|
| |

Will the data be kept for statistical purposes?

☐ Yes ☐ No

| Licensed Trade Charity: Organisation Policies and Procedures | | | |
|---|---|---|---|
| **IT POLICY** | | | |
| Effective Date: | 15th March 2019 | Title: Data Protection Policy | |
| Supersedes Date: | 8th March 2019 | | |
| | | Originator | Matt Smith / Adrian McGarry |

***Legal Basis (Appendix B)***
***Please refer to the Legal basis descriptions document for help and guidance***

## Legal Basis for holding Data

Process name: _____

Process owner: _____

To complete this form read the short description of each legal basis in the appendix. Choose one that you think could apply to your process and then complete the questions for that basis. As you go along tick off one box under the basis for each correct question. The correct answer to a question is marked with a * on the questions form

If you end up with a tick in a green box then you should select that basis as your basis of processing. If you do not get to a green box then try a different legal basis.

***Data Protection Impact Assessment (Appendix C)***

## Data Protection Impact Assessment

Process name:

Process owner:

Whose data is being collected?
e.g. Students, staff, beneficiaries etc.

What data is being collected?
e.g Name, address, contact details etc.

Does this data include special categories?

☐ Yes ☐ No ☐ Unsure

Why do we as an organisation need to collect this data?

## VII Version control log

| REVISION NO. | REASON FOR REVISION | **EFFECTIVE DATE** |
|---|---|---|
| **000** | **First Issue** | **1 Aug 2002** |
| **001** | **Re-draft** | **23 Apr 2006** |
| **002** | **3rd Issue** | **2nd July 2009** |
| **003** | **4th Issue** | **5th July 2011** |
| **004** | **5th Issue** | **9th October 2012** |
| **005** | **6th Issue** | **17th July 2013** |
| **006** | **7th Issue** | **17th July 2014** |
| **007** | **8th Issue** | **14th April 2015** |
| **008** | **9th Issue** | **7th July 2015** |
| **009** | **10th Issue (Retention of data for Medical & SEN** | **15th Jan 2016** |
| **010** | **11th Issue (obsolete URL changes)** | **14 March 2016** |
| **011** | **Change to SEN data retention under principle 5 Amendment to dates Amendment to principle 5** | **23 May 2016** |
| **012** | **New DPA and GDPR laws** | **1 Nov 2016** |
| **013** | | **22 June 2017** |
| **014** | **Changes to text** | **25 May 2018** |
| **015** | **Annual review** | **08 March 2019** |
| **016** | **Change of DPO** | **15 March 2019** |

Effective Date: 15th March 2019
Reviewed no later than: 14th March 2020