
# Encryption

## Encryption

Encryption is a process of encoding a piece of information so that it cannot be understood. It can only realistically be decrypted using a secret key. (https://en.wikipedia.org/wiki/Encryption for more). Encrypting data helps reduce the risks of a data breach, because if encrypted data is lost, it can only be read if you have the key. As long as the key is secret and secure, your lost data is unintelligible to anyone else.

There are different processes (the algorithm) that are used to encrypt data. AES-256, mentioned below, is one.

## Lamplight data is encrypted at rest

Lamplight data is stored on an AWS Aurora database, which saves the data in an encrypted form using AES-256. This means that the data on the underlying hard disks is encrypted and requires the key to read it. Data in transit with the database systems is also encrypted using AES-256.

File data is stored on S3, and again all data is encrypted within the private S3 buckets, using server-side encryption.

## Lamplight data is encrypted in transit between our servers and your browser

Lamplight only uses https – the final 's' stands for secure and means that the browser and our server send information between each other in encrypted form. This means that the data travelling across the internet cannot be read as it travels through Internet Service Providers etc. to get from you to us.

The SSL certificate also provides some measure of certainty that you are communicating with Lamplight, not some imposter that wants to trick you into handing over your login details or your data.

## What you need to think about

Once data is in your hands, you are responsible for encryption. There are four major aspects that you need to consider:

1. Downloading data from Lamplight

All tables in Lamplight can be downloaded into a .csv file. When you do that, you now have the data on your hard disk. Is your hard disk encrypted? Do you securely delete it?

2. Taking your own backups

You can also request a complete backup of your system, which is a download of your entire Lamplight system. Where do you save that file? Is it encrypted?

3. Sending us data for migration

If you are sending us data, you should ensure that you send it securely, over encrypted channels. You can send Lamplight a file through the system, a feature we provide for this exact reason. You should never email Personally Identifiable information, there are no guarantees that it is secure, and a high chance that it is not.

4. Error reporting

Sometimes you may experience a problem with Lamplight and need to contact us for support. If you wish to email us a screenshot, or details about the problem, please ensure that you do not send any personally identifiable information. Take the screenshot to avoid such information, or edit the image to blank it out. If you need to refer to a particular profile or other record, send us the ID, not the name (which is more helpful for us anyway).

**Some resources and further comments**

Window 10 Pro includes BitLocker, which can encrypt your hard disk and any external disks (e.g. backup disks, USB keys etc). Non-profits can get very affordable licenses from tt-exchange https://www.tt-exchange.org/

Some anti-virus products include the ability to create encrypted folders on your existing drive that you will have to provide an extra password for to access.

Some anti-virus software also provides a 'secure delete' function that ensures that files are properly overwritten on disk, instead of just being put in the recycle bin, or flagged as deleted without really being so.

Encryption is hard. There are some older encryption algorithms that are no longer considered secure. It is a near universal recommendation that you do not try and do it yourself. Use up-to-date, well-known products for encryption.