

**Encryption Basics**

Updated September 2021

Version 2.0

**Contents**

[**What is Encryption?** 3](#_Toc83982966)

[**Uses of Encryption** 3](#_Toc83982967)

[**In Transit and At Rest** 3](#_Toc83982968)

[**Types of Keys** 4](#_Toc83982969)

[**Secure Browsing** 4](#_Toc83982970)

[**Secure Email** 4](#_Toc83982971)

[**Who can decrypt?** 4](#_Toc83982972)

[**End-to-End Encryption** 5](#_Toc83982973)

[**Password Managers** 5](#_Toc83982974)

[**Don’t Forget Your Password!** 5](#_Toc83982975)

# **What is Encryption?**

If you write something down that is private, you might worry that someone else is going to read it. If you give the message to someone to pass on to another person, the risk of the wrong people reading that message increases. This is the same with stored data and messages we send electronically.

Encryption encodes data or messages so that they can only be understood by the person you intend to receive it. Encryption can be used for data whilst it is stored (at rest) or during transmission. It does not prevent someone from intercepting a message or accessing the data, but it prevents them from being able to understand or read it.

Encryption uses a set of rules (algorithm) to scramble data (encrypt) and uses an encryption key to unscramble (decrypt) the information. An encryption key is a piece of information used by the software algorithm to encrypt data.

# **Uses of Encryption**

* Encrypting data stored on a hard disk. This is important if a device holds sensitive information as encryption will make information unreadable.
* Encrypting an email when sending sensitive information to a colleague.
* Encrypting a document, such as a spreadsheet, to prevent unauthorised access.
* When a website uses HTTPS the information being transferred is encrypted. This means that if the connection is intercepted, the information will be unreadable. Secure connections are shown by a padlock at the start of the address bar.
* Wi-Fi encryption to protect your network.

Chromebooks, iPhones, iPads, Android phones, Macs, and some Windows machines, store their data on your local devices in encrypted form. It’s decrypted after you sign in with your PIN or password.

# **In Transit and At Rest**

When you access online accounts, vendors like Microsoft and Google use encryption to secure data ‘in transit’ to ensure that your connection remains private. This prevents internet service providers and others using the same Wi-Fi network seeing or intercepting your communications.

Microsoft and Google also use encryption to secure saved and stored data, known as data ‘at rest’. This means criminals accessing the drives containing the data, wouldn’t be able to read your data.

# **Types of Keys**

Encryption keys are used to lock (encrypt) and unlock (decrypt) information and these keys are generated with random number generators, or computer algorithms.

* **Public Key (or Asymmetric Key):** The encryption (senders key) is published and available to anyone with the receiving party having access to a different decryption key.
* **Private Key (or Symmetric Key):** The encryption (senders key) and decryption (receivers keys) are the same.

Public keys can be exchanged safely, private keys are not shared.

## **Secure Browsing**

When you browse the internet, your browser, and the website you are accessing exchange their **public keys** and then encrypt data using their **private keys**. Both sides can decrypt the information they receive from the other end.

Certificates verify the identity of websites and they are issued by Certification Authorities once the identity of the applicant has been checked. Once your browser has verified the authenticity of the site and the strength of the encryption, it places the padlock in the address bar.

## **Secure Email**

When emailing, messages are encrypted using the sender’s private key. The recipient can use the sender’s public key to decrypt and read it. Users can use their own private key to encrypt a reply.

# **Who can decrypt?**

Since Microsoft and Google hold the encryption keys, their employees can see your data (emails, documents, and files etc). Rogue employees can and have accessed data they shouldn’t have, and encryption doesn’t protect you if the person accessing the information has the keys.

In addition, if a hacker accessed Microsoft’s or Google’s systems and obtained the keys, they would be able to read everyone’s data.

Therefore, it is important to carry out effective due diligence on your suppliers and their security. This is a key requirement of data protection legislation and a fundamental part of safeguarding your school community.

# **End-to-End Encryption**

End-to-end encryption means that your provider will not be able to see the contents of your messages. They do not hold a key that unlocks your private data. Only you and the person you’re communicating with hold the key to access that data. Emails can be end-to-end encrypted, but this is not commonly used. End-to-end encryption is most commonly used for chat apps.

# **Password Managers**

It is recommended that if you are using a password manager, this is end-to-end encrypted. This means that the company cannot access your password vault and the information is protected by a secret only you know. Examples of end-to-end encrypted password managers are:

* [1Password](https://www.anrdoezrs.net/links/3607085/type/am/sid/711656/https:/1password.com/)
* [BitWarden](https://bitwarden.com/)
* [LastPass](https://lastpass.wo8g.net/c/156932/565400/8692?subId1=htg&subId2=711656&sharedid=&u=https%3A%2F%2Fwww.lastpass.com%2F)
* [Dashlane](http://www.tkqlhce.com/click-3607085-12177397-1428426211000?sid=ct711656)

# **Don’t Forget Your Password!**

Just remember that with end-to-end encryption the only person with the ‘key’ is you! If you lose your decryption key, most often a password, you lose access to your data. Some companies don’t end-to-end encrypt your files and backups for this reason, allowing them to have the key, is like giving your neighbour a spare to your house. When you need to, the company can reset the password for you.