Using MailChimp securely

As a government user you share the responsibility to keep information safe and to work securely. This guidance will help you use MailChimp securely.

MailChimp is an email service for sending automated messages, marketing emails and targeted campaigns. MailChimp lets you send notifications to clients, customers and third parties.

Securing your account

Secure your MailChimp account by using:

- a password made up of 3 random words
- two-factor authentication
- a secure (HTTPS) connection using a modern browser

Contact your MailChimp administrator if you:

- think someone may have accessed your account
- lose a device that can access your MailChimp account (you should also change your password)

MailChimp may do an additional security check if you log in from somewhere different. Set up SMS verification in case they ask.

Protecting your data

To protect your data when using MailChimp, make sure you:

- don't use MailChimp to store or send sensitive, personal, or other high value data (like commercial or financial information) that could cause harm if lost or exposed
- sign up to their Data Processing Agreement
- manage users so they can only access what they need

When using MailChimp, you should also be aware that all content can be:

- disclosed publicly under the Freedom of Information Act
- exported and viewed offline by your administrators
- subject to legal requests to share data by courts, government agencies, or parties involved in litigation in the US

MailChimp include a Data Processing Agreement for European customers to provide protection in line with European data protection requirements. You own the data you put in MailChimp, and their technical security is similar to other popular public cloud services.

Managing your information

Sometimes you need to refer back to information in MailChimp. As a civil servant, you also need to keep save a permanent record at regular intervals or at the end of a piece of work.

Make sure you don’t lose content by:

- creating a permanent record of shared information at regular intervals or at the end of a piece of work
- exporting data to your document storage or email service to capture important discussions or decisions (name the data so it can be found later)

You can export data from MailChimp by:

- copying and pasting the text (while noting the date)
- cc’ing outbound messages to an account where they can be captured
- asking your administrator for an export
- exporting individual mailing lists

Getting started

Ensure your account looks official and similar to other government MailChimp accounts by:

- setting your username to your primary corporate email address
- use a recognisable profile photo

Send messages from the right email domain. To use your existing domain you must both verify and authenticate it in MailChimp or your email may go to recipients’ spam folders. Contact your IT team to help set this up, as they will need to make changes to their email domain setup.

Think about how information might look in public if it were disclosed more widely than the mailing list to which it was sent.

Getting help

For help using MailChimp, you can:

- access the MailChimp knowledge base for guides and videos
- find your team owners or administrators (look under Account - Settings - Users to find the admin or owner’s name)

MailChimp offer support through a:

- support page
- twitter feed
- status page

You may also access further support from your internal IT team (if you have agreed a support arrangement with them).