

Anti-Spam and MCD policy.

November 2023 V3.0

INSPIRED THINKING GROUP

teamitg storyteq deployteq

Anti-Spam and MCD policy

Nov 2023 V3.0

ITG Group provides a large number of services through electronic communications mainly email and SMS. To make sure these channels of marketing are received and wanted by customers, we have a strict compliance code that makes sure these communications are not classed as spam.

This policy is designed to guide users of Team ITG multi-channel marketing services through best practice in campaign deliverability and how to follow the ever-changing rules that Internet Service Providers (ISPs) have to create. These rules are created in order to combat the growing problem of spam through unsolicited or malicious messages sent in large numbers across a multitude of platforms. It is no longer acceptable to simply target a large volume of customers for electronic communication without a legal reason for contact and a good

knowledge that the data being utilised will return engagement. Getting this wrong can lead to being marked as 'spam' by ISPs, which will hinder further campaigns and could end up with an IP and sender domain being blacklisted and unusable in the future.

Team ITG can guide and assist any client or user of their services in order to get the best possible engagement from customers and make sure messages are delivered and read.

Anti-Spam and MCD Policy Anti-Spam and Multi-Channel Deliverability

INSPIRED THINKING GROUP

teamitg storyteq deployteq configteq

Deliverability Strategy

A good strategy is essential to the successful deliverability of any campaign, whether this be with prospective or existing customers. Team ITG has dedicated Customer Relationship Management (CRM) teams that can guide, assist and create a successful strategy for any campaign. This policy will aim to cover the basics and lay down guidelines to help in the deliverability of a successful campaign, however further assistance should always be sought if unsure as there are often legal implications if you do not following the latest data protection or ISP-driven rules regarding contact to customers and anti-spam legislation.

A good strategy should start with the objectives, some examples are:

- acquiring new customers and enhancing sales
- converting prospective customers to buying customers
- building customer relationship through additional offers and promotions
- retaining loyal customers
- enhancing customer satisfaction and brand loyalty
- re-engaging lost or lapsed customers

INSPIRED THINKING GROUP

Anti-Spam and MCD policy

Nov 2023 V3.0

Deliverability – the key to success

Deliverability is very important in building successful engagement with customers; if they haven't read a message, how can they engage with the campaign? Often ISPs mark messages as spam based on behavioural metrics, which are based on whether the recipient marks the emails as spam or deletes them immediately. This means that the quality of data and sending strategy is essential. The content of emails is also important as often key indicators are used to mark content as spam or malicious, further

guidance on message best practice can be found in part 4.

There are many considerations when creating a deliverable strategy, they include clicks, opens, conversions and bounces. All of these factors can affect the campaign but one of the key factors is bounces, explained in the next section, these are when an email has not been delivered and therefore an intended recipient has not received the intended message.

Bounces

Bounces are often the first sign of either success or failure of an email campaign, especially when contacting prospective customers, or customers who have not had any prior engagement.

The different types of bounces are detailed below with the potential error type and what that indicates.

Bounces are a key indicator of a bad data source (hard bounce) or a reputational issue with an ISP (soft bounce), facilities can be provided by the Team ITG

CRM team to avoid bounces on campaigns through email verification software. This helps customers get maximum engagement by verifying email addresses before a campaign is sent; more information can be provided by your Team ITG account team.

Verification can also be conducted for other channels of communication, but advice would need to be sought through an Team ITG CRM team on the best strategy and method.

Type of bounces	Hard Bounces (Indicates an invalid email address)	Soft Bounces (Could be temporary, or categorised as one of the types below)	Ignored (Temporary message)
Reason for Bounce	<ul style="list-style-type: none">• User unknown (invalid address)• Unreachable• Account disabled• Refused (classed as spam)	<ul style="list-style-type: none">• Invalid domain• Unreachable• Mailbox full• Account disabled• Refused	<ul style="list-style-type: none">• Out of office• Technical error

Data explained

The key to a good strategy is having data that can be used legally and will return engagement. Often the marking of spam is enacted when the user, or 'data subject', does not want to receive any

communication of this type, and will therefore mark as spam, complain about contact or report the messages to a data protection authority.

Anti-Spam and MCD policy

Nov 2023 V3.0

Data protection implications

Any sending of messages directly through Team ITG services or systems must comply with the relevant data protection legislation for the geographical location where the data subjects are located, for example, within the EU, this is GDPR.

On the whole, recipients of messages, "data subjects", must only be contacted when the sender has a legitimate reason for engaging with that data subject. Under GDPR there are 6 legal reasons. These are currently some of the strictest rules and are a good way to gauge if you have permission to contact a data subject:

- **Consent** - the data subject has given clear consent for us to process their personal data for a specific purpose;
- **Contract** - the processing is necessary for the fulfillment of a contract, or because the data subject has asked us to take specific steps before entering into a contract;

Data sources explained

As mentioned above you need to abide by appropriate legislation in order to protect yourself, as the data controller and also the data subjects' legal rights.

There are many different types of data sources that will help in delivering a successful campaign. Some considerations before using data should be:

- data is from a reputable source and it is known what communication was given to the data subject on collection;
- ensure engaged customers have granular

- **Legal obligation** - the processing is necessary for ITG 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 ITG to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law;
- **Legitimate interests** - the processing is necessary for our legitimate interests or the legitimate interests of a third-party, unless there is a good reason to protect the individual's personal data that overrides those legitimate interests.

Any message sent that does not comply with the relevant data protection legislation may be considered spam and therefore have a negative impact on Team ITG system's reputation with internet service providers.

consent for the different channels used for communication;

- a privacy policy or terms and conditions are communicated to the data subject;
- an unsubscribe channel of communication is provided and recorded;
- all data subjects have known geographical location and so the correct data protection legislation applied;
- any rights of a data subject are considered, and processes are in place to deal with these after a campaign is sent.

Anti-Spam and MCD policy

Nov 2023 V3.0

A data controller must consider what was communicated to the data subject on collection. Therefore, data from the following sources should be treated with caution:

- **purchased data** – Data must be able to be traced back to its point of collection in order to ensure its authenticity and allow the data controller to make an informed decision on what channel of communication can be used. A reputable re-seller will provide this, with guidance on how the data can be used;
- **data harvested from the internet** – Often personal data can be sought through cookies and other methods of profiling. A data controller must ensure they know what was communicated to the data subject on collection, so that an informed decision can be made on how the data can be further used;
- **data collected from competitions or sweepstakes** – These data subjects have often engaged with the competition to win a prize rather than receive further communication about a product

Deliverability and message best practice

Deliverability of your messages may depend on the following factors that will help deliver a successful campaign.

The structure of your message:

- the used proportion of pictures and text;
- the presence of both text and a HTML-version of your message;
- the spam sensitivity of your message, measured with SpamAssassin (score >1.0);
- the presence of the option to unsubscribe in every message;
- the expression is not being send from a so called 'role'-address.

The reputation of the sender, which is measured per month by:

or service. Statistics show that these types of data subject are likely to mark an email as spam and often not engage further.

All data should be tested 'cleansed' before being sent though any marketing system and have a sendex score over 7.5. Any data falling outside of this needs to be assessed and approved by the group DPO.

Remember, any data sent to a data subject without any legal reason for communication will be classed as spam, and have a detrimental effect on further communication or result in legal liability through the appropriate data protection authority.

Further guidance can be found in the Team ITG Data Protection Policy and Legal and Regulatory Policy. Team ITG can provide assistance to any clients that are unsure about the legitimacy of a contact channel and associated data. For further information please contact dataprotection@teमितg.com or your Team ITG account team.

- the domain which is included in the email address of the sender and reply email address;
- the domain which is included in the reference of your expression.

The quality of our database, which is measured per month by:

- the ratio between active and inactive members (CTO > 20%);
- the number of complaints which are registered (<0.1%);
- the amount of bounces which are registered (<1.0%);
- the amount of unsubscriptions which are registered (<0.1%);
- the presence of role-addresses (<0.1%);

Anti-Spam and MCD policy

Nov 2023 V3.0

Deliverability and message best practice

Further good practice:

- avoid unnatural enrichment of your database through the merging of purchase of data with engaged data.
- the gathering of email addresses should be through a Double Opt-In process
- authentication of your sender domain (SPF, SDF, DKIM and DMARC) is important
- do not send messages containing

pornographic, racist, discriminating or offensive material

- sending of your messages is conformant to (local) legislation

Team ITGs dedicated CRM team can advise and guide customers and service users through any of the above, along with how best this can be configured and tested.

Assistance and guidance

As mentioned throughout this document, Team ITG has dedicated teams that can help and assist on all aspects of campaign delivery.

Any user of Team ITG systems or services must comply with the required legislation and avoid sending communications that are known to breach ISP spam rules and regulations.

Guidance on data protection rules and regulations can be sought through the Team ITG data protection team on Dataprotection@teamitg.com.

If you have been the victim of spam and believe that it

originates from a Team ITG system or service, please contact the Team ITG information security team on infosec@teamitg.com and this will be fully investigated. Alternatively, you have the right to report suspected spam or nuisance communications to the relevant data protection authority;

UK through <https://ico.org.uk/make-a-complaint/nuisance-calls-and-messages/spam-emails/> or in the Netherlands <https://www.acm.nl/en/contact/reporting-spam-acm>.

Policy review and approval

This policy will be reviewed annually or with any major change in legislation or practice.

It is approved and monitored at a board level and reported on through internal and external audits, where applicable.

Any questions or queries should be sent to:

ESG@teamitg.com

Effective date	Version	Owner	Changes
June 2021	V1.1	Chris Egerton	Published version on site
November 2022	V2.0	Chris Egerton	New ESG Framework
November 2023	V3.0	Chris Egerton	Annual Update