



# **Email Marketing Council**

## **Best Practice Guidelines**

27 July 2004

# Contents

1.0 Introduction .....	3
2.0 Collecting & Managing Data.....	4
2.1 Data collection.....	4
2.2 Data hygiene .....	8
2.3 House Files .....	8
2.4 Renting Lists – ‘Host Mailing’ .....	9
2.5 Appending Data.....	10
3.0 Email Campaigns.....	12
3.1 Key Issues.....	12
3.2 Campaign Hints & Tips.....	14
4.0 Standard Metrics for Measurement & Reporting .....	20
5.0 International Issues.....	20
5.1 Transferring data outside the EEA .....	20
5.2 Emails received outside the UK.....	20
6.0 Complaints and Dispute Resolution .....	22
APPENDIX A. Legal and other regulatory requirements.....	23
i. Summary .....	23
ii. UK Data Protection Law.....	24
iii. Distance selling regulations .....	25
iv. E-Commerce Regulations.....	26
v. Privacy and Electronic Communications (EC Directive) Regulations .....	26
vi. The CAP Code.....	27
vii. Bibliography .....	29
APPENDIX B. Insights into Deliverability .....	30
i. Individuals controlling delivery .....	30
ii. ISP Blocking/Filtering.....	30
iii. ISP user settings.....	31
v. Corporates controlling delivery .....	31
vi. Filtering Software.....	31
vii. Real-time Black Lists (RBLs) .....	32
APPENDIX C. Glossary .....	33



## 1.0 Introduction

The DMA's goal in developing these guidelines is to:

- help stimulate the positive development of email as an effective marketing medium;
- reinforce the key legislative issues that clients should be aware of when using this medium;
- share examples and practical advice in terms of how clients can maximise their results from using this medium;
- by doing so, play a role in terms of raising the standards within this industry and in combating the increasing prevalence of spam; and
- provide practical advice about complying with working practices and standards of the Internet industry.

They focus on marketing by email as it is normally understood, as opposed to marketing by text, video or picture messaging and have been put together by the UK's leading email marketing proponents, who have shared their expertise in order to provide a framework and guidance for the effective and proper utilisation of email marketing.

These Guidelines are not a substitute for the relevant codes, for instance the DMA's Direct Marketing Code of Practice and the CAP Code of Advertising, Sales Promotion and Direct Marketing. Nor are they advice on the relevant laws, most importantly the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("the 2003 Regulations"), more details of which are in the Appendix. All these must of course be complied with in any event and if members are ever in doubt as to whether they are code or law compliant, further advice should be sought. Compliance with the contract and acceptable use policy (AUP) of the ISP used is also required/expected.

The purpose of these Guidelines is rather to help marketers using this highly effective marketing medium to achieve the higher goal of "Best Practice".

For ease of reference we have included at the end of the Guidelines a "Glossary" of terms. In some cases these defined terms start with a capital letter. For instance "Data User" is defined as "an organisation making use of either its own data or of data obtained from other sources for any direct marketing purpose".

It may help readers' quick understanding and assimilation of these Guidelines to start with the Glossary.

## 2.0 Collecting & Managing Data

Good quality prospect and customer data is the cornerstone of a successful email campaign. However there are many issues to be addressed to ensure that best practice is achieved in the collection and use of data. This section provides a guide through these key issues.

### 2.1 Data collection

When collecting personal data which includes an email address, Data Users should:

- comply with the "fair processing" and other relevant requirements of the Data Protection Act 1998 (see Appendix A for more information on this);
- only ask for information that is reasonably necessary for the purpose for which the data is being used;
- have a clear Notice providing all requisite data protection notices and a link to, or full details of, a suitable Privacy Policy at the point of collection;
- comply with all relevant codes;
- gain positive consent to send Unsolicited Commercial Email Messages (for example with the use of an 'Opt-In' check box), unless the exception below applies:
  - Where 'Soft Opt-In' applies, follow the collection procedure described at 2.1.1 below, ensuring that the opportunity to opt out of receiving future unsolicited marketing emails appears with reasonable prominence and is easy to take up, for instance by way of checking an opt out box as opposed to having to send a separate email, send a request by post or having to make a telephone call.
- comply fully with the requirements below of 2.1.2 Data Protection Notices and 2.1.3 Privacy Policy; and
- send a confirmation email after subscription which a) clearly confirms what the person has signed up for and what data they provided b) gives them the chance to correct any incorrect data and c) says something like 'if you've signed up in error, do *this* (e.g. one click, easy to use) to cancel your registration and d) includes a telephone number to call (customer service line) if the subscriber has any concerns.



The 'harvesting' of email addresses from websites, emails and other sources in the public domain without seeking individual consent is likely to involve contravention of the Data Protection Act 1998 ("the DPA").

### **2.1.1 Soft Opt-In Exclusion**

Unsolicited Commercial Email Messages may be sent to "individual subscribers" without positive consent who are prospects or customers of the Data User; and the email address has been gathered in the course of the sale or negotiations for the sale of a product or service to the prospect or customer.

In this case, the Data User must have notified the individual at the point of data capture that they would like to send the individual emails marketing the Data User's own 'similar products or services'. The individual must have been given the opportunity of opting out of this at the time of data collection and on every subsequent marketing email and declined to do so.

"Similar products and services" and "in the course of the sale or negotiations for the sale of a product or service" are not defined in the Regulations. The Information Commissioner's Office ("ICO") has published Guidance, however, on how these phrases should be interpreted.

As regards "negotiations for the sale of a product or service" ("Negotiations") the ICO accepts that it may be difficult to establish when these may be starting. However, it goes on to state that, where a person has actively expressed an interest in purchasing a company's products and services, this can be regarded as Negotiations. On the other hand, the ICO would not regard as Negotiations a situation where cookie technology is used to identify a person's area of interest when they are browsing a website, unless that person has expressly communicated their interest in purchasing available products or services, for example by requesting a quote. The ICO would also not regard as Negotiations an email asking a retailer whether they are opening a branch in a particular town.

On the meaning of "similar products and services", the ICO indicates that a purposive approach is appropriate. The intention here is that an individual does not receive promotional material about products or services that they would not reasonably expect to receive. For example, someone who has shopped on-line at a supermarket's website (and has not objected to receiving further email marketing from that supermarket) would expect at some point in the future to receive further emails promoting the diverse range of goods available at the supermarket.

### **2.1.2 Data Protection Notices**

When collecting an email address (online and offline), the information (data protection notices) below should be prominently displayed (as a 'notice') at the point of collection:



- clearly identify the Data User, including the full corporate name and postal address details (which must include the registered office of the Data User if it is a registered company and may also include a trading address);
- provide clear and unambiguous details of the purpose or purposes for which the e-mail address (and any other personal data being collected) is to be used. In particular:
  - i. individuals must be clearly made aware of any intended use of the email address provided, including any proposed use of the address for the purpose of sending email marketing messages promoting other products or services of the Data User.
  - ii. if such use is proposed, full details of the likely subject matter of the future messages should be given.
- if there is a desire to share the email address collected with other divisions within the Data User company, the ICO's Guidance indicates that it is a question of considering the reasonable expectations of the individual. If a company trades under several different names, particularly where those names are strong brands, it cannot be assumed that an individual who agrees to receive marketing emails from one trading entity is agreeing to receive marketing emails from other trading entities. They may not even be aware of any connection between different trading names. In such cases it will be important to ensure that the individual is made aware that they will receive Unsolicited Commercial Emails from all the company's trading names when they opt in to receiving marketing from that company;
- there may be a desire to share the email address with other limited companies within the same group as that of the Data User. If so the relevant company names and postal addresses should be given, the country of incorporation of the other group companies in question, a description of their products or services, and the relevant brand names, together with a clear description of the uses the other group companies would like to make of the email addresses. The individual should then be given an opportunity of specifically indicating their agreement to their email address being passed to that other company and to receiving Unsolicited Commercial Emails from that source;
- state any other means by which data regarding the individual is collected, including cookies, clear-gifs or other similar indicators, as well as an explanation of the purposes for which that data is to be collected. There should be an explanation as to why those particular methods of data collection are being used given with a clear and easy to identify opportunity to refuse the operation of these indicators; The IAB's allaboutcookies site ([www.allaboutcookies.org](http://www.allaboutcookies.org)) is a source of further information when considering the implications of cookies within UK legislation;



- state whether the requested personal data are necessary to the transaction between the individual and the Data User, or is voluntary, and the consequences of failing to provide the requested information (for example, if the individual will not be able to access the service in question without the use of a cookie); and
- how to unsubscribe from any mailing list.

### **2.1.3 Privacy Policy**

Given the nature of these Guidelines, the disclosures suggested above naturally focus on transparency, at the point of data collection, as to the likely future uses of email addresses. There will doubtless be other data protection-related notices that the Data User will wish to make, as a matter of law and best practice.

Since it may be inconvenient to provide this more extensive data protection notice at the point of data collection, general data protection Best Practice allows these other notices to be made elsewhere, by way of a clear and easy to understand "Privacy Policy".

This is on condition that if the email address and other personal data are being captured on-line, the Privacy Policy will be accessible in one click by way of a prominently flagged link above the submit button (as opposed to a "Privacy Policy" link in amongst various other general links to Terms and Conditions etc, or in a sidebar or only visible after scrolling to the very bottom of a web page). It should also be clearly accessible via a link from every email delivered.

If the data is being collected off-line, the Privacy Policy should be set out, as a matter of Best Practice, in full and attached to the material (such as an application form) used to collect the data.

Data Users will need to take care to ensure that their Privacy Policy is tailored to their particular needs, the expectations of their prospects and customers and consistent with their notification with the Information Commissioner's Office. The Privacy Policy should also set out the complete policy of the Data User with regard to personal data, and should therefore include, in a manner that is completely consistent with the data protection notice given at the point of collection, the policy as regards e-mail address use. Please refer to section 19.22 of the DMA Code of Practice for further information.

Data Users will need to take guidance on the terms of their own particular privacy policy.

## **2.2 Data hygiene**

Good list hygiene practices, ensuring the quality of customer and prospect data, are critical to developing consumer trust and also help facilitate message delivery.

Data Users should develop a list hygiene policy that outlines the procedures which will be used to address such issues as: reply handling; the processing of unsubscribe requests; and the appropriate handling of bounce-backs, including communicating unsubscribe time frames to each recipient; suppression of known invalid addresses; and address format validation.

The goals of the policy should be:

- to reduce incorrect, incomplete or outdated addresses to a minimum,
- to process online unsubscribe requests immediately,
- to process unsubscribe requests received offline within 10 working days,
- to inform those unsubscribing how long it will take to be effective.

Data Users should ensure that systems are in place to support the policy.

Data Users should also ensure that the individual's email contact details are "suppressed" rather than deleted upon receipt of an unsubscribe request. This should ensure that the individual's opt-out/unsubscribe request is recorded, retained and respected until such time as that individual reconsents, which overrides their previous opt-out request. Data Users must screen email-marketing lists against this in-house suppression file prior to each email marketing campaign.

## **2.3 House Files**

### **2.3.1 Existing personal data**

In order to assess a House File which include email addresses in existence before 11 December 2003 (the date of coming into force of the 2003 Regulations), Data Users should segment these as follows:

- i. Customers & prospects that have provided positive consent to the receipt of email marketing by the Data Controller and have not subsequently unsubscribed.
- ii. Existing customers with whom the Data User obtained the email address in the course of sale of a product or service and notified the individual at the point of data capture that they would like to send the individual direct marketing emails marketing the Data User's own 'similar products or services' (see 2.1.1) The individual must have been given the opportunity of opting out of this and declined to do so.



- iii. Prospects or customers who do not fall into either of the above segments.

Going forward, as a matter of best practice, and assuming all other legal requirements are met, the Data User may continue to send marketing email to the individuals in segments i. and ii. This is on the condition that:

- a. the recipient is given the opportunity to unsubscribe, using a simple means and without charge (excluding cost of transmission, provided it is not premium rate), each time an unsolicited marketing email is sent; and
- b. the e-mail's content is, in terms of the products it is promoting, within the terms of the initial data protection notices provided to the individual at the time that the email address was first captured.

In order to communicate via email with segment iii, the Data User will need to gain their positive consent to do so. Of course this should not be done by way of an email request, but by post, in person, or, within the constraints of the relevant provisions in the 2003 Regulations, by telephone, ensuring that in all such cases, a proper record of the individual's invitation or notification is kept.

### **2.3.2 New personal data**

When collecting new personal data for House Files, reference should be made to the "Data Collection" section earlier in these Guidelines.

## **2.4 Renting Lists – ‘Host Mailing’**

There are several ways that Data Suppliers may rent a list. There is only one approach that is considered to be Best Practice, this approach is known as a ‘host mailing’.

This is where a Data Supplier will, usually for a fee, send (or instigate the sending out through their normal outsourcing arrangements under a data processing agreement) email marketing to their own email database, promoting the Data User’s products and services.

In this case:

- the Data Supplier must have obtained positive consent of individuals to send such ‘host mailings’ marketing of the types of products or services of the marketer (the Data Supplier cannot rely on the Soft Opt-in Exclusion for this type of marketing);
- the Data Supplier’s email database is not passed to the Data User other than for de-duplication processes;
- the Data Supplier’s name must appear in the ‘From’ box of the email as the sender of the email; and
- the Data Supplier manages the unsubscribe process as described under ‘Data Hygiene’.



It is the responsibility of the Data Users to be satisfied as to the circumstances in which the email addresses came into the possession of the Data Supplier.

Amongst the areas of enquiry the Data User should pursue with the Data Supplier before entering into a commitment, will be:

- how and when the list was built;
- what data protection notices and privacy policies were present at the point of data collection (see 2.2.2 & 2.1.3);
- what indications were given by individuals, at the point of their email address being supplied, as to their preferences in respect of future email marketing directed to them;
- how "unsubscribe" requests, received since use of the list started, have been processed and the relevant addresses suppressed; and
- whether the Data Supplier has been otherwise legally compliant as regards the collection and subsequent use of the email addresses.

If a Data Supplier cannot provide this information and supply suitable verification and contractual warranties and indemnities, Data Users should not proceed with renting this data.

For more information on working with Data Suppliers see 2.4 'Host Mailings'.

## **2.5 Appending Data**

Appending is a complex area that requires careful consideration prior to undertaking the exercise, as it can be costly and may end up falling foul of the law.

Here are two examples. At first sight both methods appear very similar (you are appending data) but from a customer and Best Practice perspective they are very different.

Best Practice is to reach a decision on appending data based on understanding what the customer will reasonably expect to receive. The key is 'transparency'.

**Email Append:** where information about an individual held on a House File excludes an email address, but has an email address appended to it, not by way of the contact/customer providing it, but as a result of obtaining the email address from a third party source, by way of amalgamation of data. It is possible that this could be within the law, depending on how the email address was obtained in the first place. For instance the relevant individual may have volunteered it in circumstances where, as a result of the data protection notices given to the individual at the time and the consents given, the subsequent "append" is within the law. This will be provided the Data User, once in possession of the amalgamated data, complies with the further obligations placed upon him by the DPA as regards the compliant processing of that additional data. However it is not recommended best practice.



**N.B** The House File owner should be aware that a communication channel is being added to an existing customer's profile through which they may not expect to receive information and will probably perceive any communication as spam/unsolicited email.

**Data Append:** where personal data about an individual includes an email address, but has other data about that individual (for example lifestyle data) appended to it through the amalgamation of data from third party sources. it is possible that this practice could be within the law, depending on the circumstances in which the other data was initially supplied, and provided the House File owner is satisfied as to those circumstances and complies with the obligations placed upon him by the DPA as regards the future processing of that data. It is recommended that House File owner's consult the DMA Legal Department, their own legal advisers, and /or the Information Commissioner's Office to determine whether or not a particular data append is legal before carrying it out.

**N.B** In this case additional existing customer profile information is being added to an existing communication channel and, as such, may well improve the customer's communication experience by providing them with more targeted information.



## **3.0 Email Campaigns**

There are many factors that can determine the success of a campaign including the strategic purpose of the email, the content and the audience and how it is integrated into the broader marketing mix.

The following section provides best practice guidelines for the operation of an email marketing campaign.

### **3.1 Key Issues**

#### **3.1.1 Unsubscribe Process**

On every email, it is best practice to provide one of the following methods for unsubscribing:

- A URL link to click through to an unsubscribe page
- Replying to the message with unsubscribe in the subject line
- Invoking a new email to send that includes a customer ID
- A postal address for unsubscribing

#### **3.1.2 "For the time being"**

Under the 2003 Regulations, the Data User may compliantly send unsolicited marketing email to individual subscribers if the individual has previously notified the Data User that the individual consents "for the time being."

The Information Commissioner's Office indicates in its Guidance to the 2003 Regulations that such consent will remain legally valid for as long as there are good grounds for believing that the recipient remains happy to receive the marketing communications in question. The Guidance gives an example of the individual "responding positively" to previous emails (other than to unsubscribe!).

This guidance is considered suitable for Best Practice.

#### **3.1.3 From Header & Subject Line - Transparency**

The Data User (or Data Supplier in the case of a hosted mailing) must ensure that their identity is clearly stated to the individual in the 'From Header'.

The Subject Line should accurately reflect the subject, purpose and content of the message. Marketers should avoid deceptive prefixes in the Subject line, such as 'Re' or 'Fw'.

#### **3.1.4 Viral Email Marketing**

Viral email marketing describes any strategy that encourages individuals to pass on an email to others, creating the potential for exponential growth in the message's exposure and influence. Like viruses, such strategies take



advantage of rapid multiplication to disseminate the message to hundreds or thousands of people.

In theory viral marketing runs a risk of putting the individual forwarding an email in breach of the 2003 Regulations; however the view of the Information Commissioner's Office is that viral marketing does not cause significant problems, and that as long as the incentive for an individual to forward on the message is not too 'aggressive' or 'inappropriate', the practice would probably be considered acceptable.

With this in mind however, no Best Practice recommendations can be put forward for viral email marketing. Marketers will need to obtain advice from the DMA Legal Department or their legal advisers on a case-by-case basis.

### **3.1.5 Privacy Policy & Use of cookies**

In every email you should include:

- a clear link to the privacy policy of the Data Supplier; and
- a clear link and comprehensive information on the cookie policy of the Data Supplier where clear and comprehensive information about any cookie, clear gif or similar device within the email is provided, including the purpose of any storage of and access to any information stored on the recipient's terminal equipment, and an opportunity for the recipient to refuse its deployment.

### **3.1.6 Marketing to Children**

Another area that has been much discussed is that of marketing to children. Not the least of these difficulties is that there is no universally accepted definition of what age defines childhood for these purposes – different jurisdictions have defined children as anything from under 12 to under 18.

The way in which children perceive and react to email marketing communications is influenced by their age, experience and the context in which the message is framed; email marketing communications that are acceptable for young teenagers will not necessarily be acceptable for younger children. Yet there is no way to guarantee the age of any child who signs up for email marketing.

Given the general air of mistrust amongst the general public, the DMA has decided that under Best Practice guidelines, no person under the age of 16 should be the target of an email marketing campaign.

### **3.1.7 Host Mailings – Working with Data Suppliers**

The section below addresses the relationship between a Data User and Data Supplier when a Data User is running a host mailing. It is incumbent on the Data User to take full responsibility for the email activity booked. Once due



diligence is completed (see 2.4 Renting Lists), the Data User should agree the following processes with the Data Supplier:

*i. Written approval/ confirmation process:*

- Insertion Order (IO) to include some or all or the following: cost, segment information, quantity, dispatch timing, position, and number of words per email;
- format agreement (text and/or HTML);
- content checked for consistency with original notice at point of data collection; and
- any requirement for copy clearance from the CAP copy advice team, the DMA Legal Department or other expert advisers.

*ii. Message delivery process:*

- The Data Supplier must provide the individual with the opportunity, using a valid address, to unsubscribe from any future communication from that list, using a simple means and without charge. This can be an email address, but it should not be a telephone number, even if it is freephone; and
- clearly identify the Data Supplier, including its full corporate name and registered address if a company, and a trading address if different and if desired.

*iii. Post campaign process:*

- Certificate of delivery to be issued within an agreed timeframe following the dispatch of the campaign; and
- contingency plan for under delivery, linked directly to invoice: net names charging basis / net names for under delivery.

## **3.2 Campaign Hints & Tips**

### **3.2.1 Personalisation & Relevance**

The use of personalisation with an email provides an opportunity to communicate with individuals at a more intimate level. Most email deployment technologies allow personalisation to be included anywhere within the body of the email as well as within the subject line.

To maximise the benefits of personalisation it is important to clearly review the type of information the Data User would like from individuals at their point of registration. As a minimum, Data Users should aim to capture their first and last name. Other data, such as date of birth and postcode, may be of equal importance depending on the nature of the Data User's business.

In addition to personalising the email with data captured with positive consent, the opportunity exists to draw upon other relevant data that may be held, including previous purchase history, enquiries or preferences. By referring to



these within the email the Data User is again able to increase the level of relevance to the recipient.

More advanced email deployment technologies can also provide for the delivery of dynamic email content whereby the content and images of an email is personalised to each individual's specific profile.

### **3.2.2 Email Format**

There are currently three formats of email. The type of email that can be received will depend on the email software package on the recipient's computer.

Early email software provided only for a **plain text** email. This type of email provides for black text only and any links to a web site appear as a complete URL such as <http://www.dma.org.uk/DMA/default.asp>. To reach the web site the URL has to be copied in its entirety and entered into an internet browser. The individual cannot click directly from the URL to reach the designated web site. Plain text is typically found within early versions of Lotus Notes.

**Rich text emails** are an evolution of plain text. These software packages allow for both coloured and variable fonts. In addition any links to a web site contained within the email can be clicked on directly rather than having to copy and paste. By clicking on a URL the internet browser on the computer is launched which takes the individual directly to the web site. Rich text emails are found in early versions of Microsoft Outlook and AOL.

The most advanced type of email software provides for an **HTML email**. An HTML email has the same look and feel as a web page. It can support images (including animation) whilst the functionality is the same as rich text. By clicking on a URL the internet browser on the computer is launched which takes the individual directly to the designated web site.

HTML emails have emerged as the popular choice for email marketing given that their more dynamic appearance can often pull a higher response rate than plain or rich text emails.

#### **How do I know what Email Format my Customers have?**

There are two standard methods of determining the type of email an individual can receive.

Firstly, at the point of registration the individual could indicate whether they wish to receive a text or HTML email. For those individuals who understand their email software well enough they can pre-determine the format of the email. Similarly some individuals may prefer a text email as opposed to an HTML email; typically individuals who read their emails offline often prefer this.

Secondly, some email providers overcome the guesswork of whether the individual can receive a text or HTML email by sending both emails

simultaneously in a format referred to as “Multi-Part”. The individual's computer will then recognize and display the optimal email format.

### **3.2.3 Targeting**

Targeting is an essential requirement of any marketing activity. To be able to reach the correct audience with the correct offer is the primary objective.

For traditional forms of marketing this can be an enormous challenge, printing one version of a brochure can be achieved economically, printing 200 versions of the same brochure to reflect the varying preferences of individuals can be cost prohibitive.

Email, in comparison, is a lower cost medium enabling marketers to develop multiple versions of the same message depending on the preferences of customers & prospects.

This is usually facilitated by the use of dynamic content whereby the individual's preferences or previous purchase history can be used to determine the most appropriate content for the email. The majority of email providers will have the ability to deliver dynamic content based on a content library and a series of predictive or deterministic rules.

### **3.2.4 Managing Response**

One of the major benefits of email marketing is the speed of response. Often, up to 90% of responses generated by an email campaign will occur within the first 48 hours. This can provide a multi-faceted challenge to the marketer.

If the email contains any links to a web site the Data User should ensure that the web site can support a spike in the number of web site visitors that an email campaign could deliver. If recipients of an email are unable to reach a web site or web page this can have significant damage to the Data User's brand.

Data Users should remember to brief any support staff. An email campaign may be designed to drive individuals to a high street store or to call a contact centre – even if this is not a specific requirement of the campaign, it is useful to bear in mind that some individuals may prefer to enquire or purchase in person or over the phone rather than on-line.

It is likely that some recipients of the email will use the Reply button to send a message to the Data User. Typical replies can include “Unsubscribe Me”, “Send me a Brochure”, “What is my Order Status”, “I have Moved House”. In order to not become overwhelmed by the level of response appropriate steps should be taken to enable such messages to be processed in a timely fashion.

Many email-marketing providers have technology that is able to screen the replies. This technology can be used to automatically handle certain types of replies such as Unsubscribe Me. It is inevitable, however, that some replies will require a personal reply from the Data User. Steps should be taken to



ensure that these replies are directed to the appropriate department or individual and that a reasonable service level is put in place.

Finally, email responses will be generated by any of the following: invalid email addresses, incorrect domain names, ISP blocking, out of office messages to name but a few. All of these responses will need to be managed appropriately.

### **3.2.5 The Structure/Layout**

The layout of an email is as important as any other communication. An email appears in portrait requiring the recipient to browse down the page. Research suggested that a customer browses their emails before being drawn in to a particular area of interest.

Techniques to assist with this tendency to browse depend on the purpose of the email –

- Newsletters often benefit from a Table of Contents at the top of an email outlining the copy contained within the communication. The recipient can then review the Table of Contents before clicking on the Table to reach the elements within the email or web site in which they are particularly interested; and
- Promotional emails typically use more imagery and highlight the most relevant offer available to the individual at the head of the email.

### **3.2.6 Subject line**

The subject line should convey a strong call to action – a compelling subject line will draw the recipient into the email in much the same way as headlines on a newspaper entice the reader to look further. It should provide enough information for the recipient to want to know more and encourage the opening of the email.

If the email forms part of a regular communication, consider a consistent subject line such as “DMA Monthly Newsletter – June 2004”. This will allow the individual to make a rapid association with the content of the email message.

The speed and cost effectiveness of email allows for economic testing of a selection of subject lines. If there are two alternative Subject Lines, take a subset of the data, test the two Subject Lines, check the results (24 hours is normally sufficient), and then roll out the campaign with the most popular subject line.

When preparing subject lines, awareness should be given to filtering software that may determine that your email is spam based upon a set of rules applied to your subject line.

Lastly, keep the subject line to a manageable length with a maximum of 70 characters.



### **3.2.7 Above the Fold**

This is traditionally a direct mail term indicating the copy that falls above the fold of a letter – for direct mail this is nearly always the most compelling part of the offer. For email it applies to the area of the email that can be observed when the email reader is set to auto preview – in this case generally the top 50mm of the email is visible. The most compelling copy or image should appear here to encourage the individual to open the email and read on

### **3.2.8 The Size of the Email**

Given the differences in access to the internet, it is sensible to keep emails small so as not to block dial-up lines.

To reduce the size of the email, various techniques can be employed including not embedding images but serving them from an image server.

As a guideline messages should not exceed the 60k in total file size.

### **3.2.9 Frequency of Communication**

Consider frequency of communication as a vital issue for recipients, as frequency of communication has a direct correlation with the perception of marketing communications as unsolicited email/spam.

The optimum frequency will depend on the relationship between the Data User and the individual. Of course a newspaper publisher may deliver a daily email, whilst a retailer may deliver a monthly promotion.



## 4.0 Standard Metrics for Measurement & Reporting

A principal attraction of email marketing is the transparency of the medium provided by the performance metrics that can be obtained. These metrics can help track the success of a campaign, enable better targeting of the audience and help keep lists clean.

With effective software or outsourced solutions, Data Users can access a variety of data, including the standard metrics listed below. This information may be delivered in a number of ways: online in real time, as a structured report, a presentation or an Excel file. It may be provided as absolute numbers and/or a percentage of the volume sent or delivered. It should be clear whether a metric is 'unique' or 'total', for example: if an individual opens a message 5 times, this may be counted as 5 'total' opens or one 'unique' open.

### Delivery Metrics

- Emails sent
- Emails delivered
- Emails failed due to invalid email address or bounced message

### Open Rate

Data Users can detect the number of HTML emails opened. This is usually linked to the download of an image (usually a clear GIF) or a cookie.

### Click Through Rate

Data Users can record the number of individuals clicking on the links, and which links they clicked on.

### Click to Purchase\*

Data Users can correlate directly the clicks from the email resulting in transactional behaviour. From this a clear calculation of the Return on Investment (ROI) from a programme or campaign can be made.

### Click to Conversion\*

Data Users can correlate directly the clicks from the email resulting in a conversion rate for a required action e.g. clicks converting to sign-ups for a newsletter or a successful download on an offer.

\* These metrics are not standard to all software solutions and may require additional integration work with an existing website.



## **5.0 International Issues**

### **5.1 Transferring data outside the EEA**

The "Data Collection" section above indicates what data protection notices and consents should be provided if there is any possibility of email addresses being transferred outside the European Economic Area (the 25 member states of the European Union plus Iceland, Liechtenstein and Norway) for any form of processing.

As all such transfers are in any event contrary to the Data Protection Act 1998 unless certain requirements can be fulfilled, so best practice must include obtaining expert legal advice from the DMA Legal Department or your own advisor on the position before contemplating a transfer.

To provide some idea of how the restrictions work:

Individual prior consent must be obtained unless there is another lawful basis for the transfer i.e.:

- the transferee country has been designated by the European Commission as having an "adequate" level of data protection. Please see the up to date list at:  
[http://europa.eu.int/comm/internal\\_market/privacy/adequacy\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm)
- the transfer is made under a "Safe Harbor" arrangement as set up in the US where individual companies sign up to work under a self regulatory system based on EU operating guidelines. However, the US Safe Harbor Scheme doesn't currently apply to all sectors e.g. US financial services organisations cannot join;
- the transfer is necessary for the performance of a contract between the individual and the Data User or for the implementation of pre-contractual measures taken in response to a request from the individual;
- a written, signed contract exists between the Data User and the recipient of the data ensuring an adequate level of data protection. Standard recommended terms exist that are suitable for this purpose. The DMA Legal Department or other expert advisers can assist here.

It should also be noted that physical security of the data is deemed to be a requirement of safe transfer of data. For instance, it is the responsibility of the Data User to ensure that wherever its data is transferred is secured from physical theft or hackers.

### **5.2 Emails received outside the UK**

Given the medium email marketing uses, there is inevitably the prospect of email messages being received outside the UK. In the country of receipt, the laws and codes that apply to the content and deliverability of commercial email may differ from those in the UK.



The EU Privacy and Electronic Communications Directive (implemented in the UK by way of the 2003 Regulations - see Appendix A) seeks to harmonise the position across the European Union on whether prior consent is needed before sending unsolicited commercial email.

However, EU member states were given a degree of latitude in how to implement the Directive's provisions as to whether to extend the protection offered to individual subscribers to corporate subscribers. As a result of this, language differences and different drafting practices by individual member states, there will inevitably be slight, but potentially crucial differences in the ways in which individual member states transpose the Directive into their laws.

Internationally there are problems, US state courts have in certain cases applied their local laws to email messages coming out of other US states, and could conceivably take the same position in relation to emails coming from a UK based Data User.

In all circumstances it is prudent to take independent legal advice from the DMA Legal Department, other legal advisers and/ or consult the Information Commissioner's Office, as each country may operate slightly different regulations.

Under the DMA Code marketers should always screen e-mail lists against the E-Mail Preference Service if they are emailing to countries outside the EEA.



## 6.0 Complaints and Dispute Resolution

Data Users should develop a dispute resolution policy, and convey it clearly. Any complaints from individuals regarding the use of their email address, whether at home or at work, should be dealt with courteously and promptly.

Data Users, not the email service bureaus that distribute on their behalf, have ultimate responsibility for handling any enquiries and disputes regarding email delivery in a responsible and efficient manner that complies reasonably with the individual's request.

Data Users should respect individual's rights under the Data Protection Act 1998 to ask them not to process their data for direct marketing purposes. Data Users who hold data about individuals should also remember that individuals have rights under the Data Protection Act 1998 to access all data held about them (subject access requests), call for the correction of mistakes and take action in respect of any distress or damage caused by the processing of inaccurate data. Data Users in receipt of requests or complaints from individuals may wish to take appropriate expert advice on their legal obligations.

It is Best Practice to ensure that all back-office systems are set up to enable immediate suppression of an email address following receipt of an unsubscribe notice. This aspect is dealt with in more detail in the "Data hygiene" section at 2.2 above.

In the case of a dispute regarding personal data between an individual and a DMA member, the Direct Marketing Authority is available to help resolve the matter.

## APPENDIX A. Legal and other regulatory requirements

### *i. Summary*

It is important that those operating Best Practice in email marketing appreciate the minimum they need to do to ensure compliance with compulsory legal and regulatory requirements that apply to email marketing in the UK.

These include:

- (a) general UK data protection law currently contained in the Data Protection Act 1998;
- (b) specific rules for distance selling set out in the Consumer Protection (Distance Selling) Regulations 2000;
- (c) specific rules applicable to email marketing in the Electronic Commerce (EC Directive) Regulations 2002;
- (d) more specific rules applying to email marketing in the Privacy and Electronic Communications (E C Directive) Regulations 2003. In this connection readers are strongly advised to consult the DMA's summary of these Regulations and the "Guidance" to the Regulations published by the Office of the Information Commissioner in May 2004;
- (e) the requirements for email marketing in the Committee of Advertising Practice Code of Advertising, Sales Promotion and Direct Marketing ("CAP Code");
- (f) the remainder of the CAP Code (which applies to all email marketing sent in the UK);
- (g) the DMA Code of Practice;
- (h) all UK laws generally applicable to marketing material such as the Trade Descriptions Act 1968, the Consumer Protection Act 1987, the Control of Misleading Advertisements Regulations 1988 as amended by the Control of Misleading Advertisements (Amendment) Regulations 2000 to cover comparative advertising, the Copyright, Designs and Patents Act 1988, the Trade Marks Act 1994 and the Defamation Act 1952;
- (i) where email marketing is received outside the UK, relevant local legal and regulatory requirements, for instance US state laws targeted at commercial email, and state laws and regulations of other EU states where these might apply and vary from their equivalents in the UK; and
- (j) the Communications Act 2003 and in particular its provisions prohibiting "persistent misuse" of electronic communications networks.

In this Appendix we will focus only on (a) to (e) above. But we will only provide an overview. This is for general guidance only and should not be relied upon as legal advice for the purposes of any planned email marketing campaign. In such cases, separate advice should always be taken to ensure compliance.



## ii. UK Data Protection Law

This is mostly contained in the Data Protection Act 1998 (“**DPA**”).

Helpful guidance on the basics of the DPA can be found in the DMA publication "A Guide to the Data Protection Act 1998 for Direct Marketers".

In essence, however, the DPA confers rights on living individuals or “**data subjects**” in respect of others’ use of their “**personal data**” and places obligations on “**data controllers**” whenever they are “**processing**” personal data. All the terms in quotes are defined in the DPA, but in a nutshell:

- a “data controller” is any entity that makes decisions as to what is to be done with personal data;
- “personal data” is any information about any living individual or “data subject” (regardless of whether that person is resident in the UK or that person’s data is processed in a B2B or B2C context) that is capable of identifying that individual, either as it stands or when combined with other data in the possession of the data controller (some email addresses may not qualify as personal data, but for practical purposes, and as a matter of Best Practice, it should be assumed that they do); and
- “processing” in relation to personal data means obtaining, recording or holding the information or data, or carrying out any operation or set of operations on the data including:
  - a. organisation, adaptation or alteration
  - b. retrieval, consultation or use
  - c. disclosure by transmission, dissemination or otherwise making available or
  - d. alignment, combination, blocking, erasure or destruction.

The obligations on data controllers are many and various but in essence are obligations to

- “**notify**” or register with the Information Commissioner’s Office its name and address and information about its processing of personal data. The DPA requires every data controller who is processing personal data to notify unless it is exempt. The Information Commissioner’s Office statutory duty is to enforce data protection legislation and promote good personal data handling practice;
- comply with the eight data protection principles covering aspects such as data collection, use, disclosure, maintenance, security and international transfer as well as the outsourcing of data processing;



- only process “**sensitive**” personal data (such as data as to a data subject’s religious beliefs, health history, political opinions, racial or ethnic origin and sexual life) with the data subject’s explicit prior consent (“**opt in**”); and
- co-operate with the Information Commissioner's Office in connection with any enforcement action taken.

**Perhaps the key data protection principle is that requiring fair and lawful processing of all personal data.**

The underlying idea here is that data subjects should be aware at all times of who is processing their data and for what purposes. From this flow the principal data subject rights to:

- obtain, by way of a “**subject access request**”, details of all personal data relating to them held by data controllers;
- require correction of any errors in that data;
- seek damages in respect of any inaccurate data held about them which is likely to cause them damage or distress; and
- require that all processing of their data for marketing purposes cease.

The obligation to provide information to the individual extends to data controller A coming into possession of personal data about data subject B from entity C. Entity C should already have obtained data subject B's consent to sharing B's data with A. A is then legally obliged, unless it would involve "disproportionate effort", to notify B that A has B's details. Also, depending on the circumstances in which C first captured B's details and the use A wishes to make of these, A must give B the opportunity to opt into or out of A's further use of that data. There may be circumstances in which this can be compliantly done by way of A's first marketing contact with B.

### ***iii. Distance selling regulations***

The Consumer Protection (Distance Selling) Regulations 2000 apply to any “direct response” email message to which a consumer can respond by ordering a product or service. They contain three main strands:

- disclosure requirements, for instance as to the identity of the supplier, the characteristics of what is being offered and the price;
- fulfilment requirements, for example within 30 days unless otherwise agreed; and
- a cancellation right for most products, exercisable unconditionally, in most cases up to seven working days starting the day after delivery.

All of these requirements will impact on the information to be contained in the email message.



#### ***iv. E-Commerce Regulations***

Unlike the 2000 Distance Selling Regulations, the Electronic Commerce (EC Directive) Regulations 2002 largely apply in a B2B as well as a B2C context.

For email marketers, their significance is that they impose more data protection notice obligations that have a direct impact on the content of the email message.

Perhaps the most important one of these is the obligation on the sender of an “unsolicited commercial” email to ensure that it is “clearly and unambiguously identifiable as such as soon as it is received”.

Even if the commercial email is solicited it must still be clearly identifiable as such somewhere in the message. Also, both solicited and unsolicited marketing emails must clearly identify the person on whose behalf the communication is made, any promotional offer, competition or game mentioned and any conditions for participation, all of which information must be “easily accessible and presented clearly and unambiguously”.

Other provisions require, in a direct response context, that unless non-consumers have agreed otherwise, the email message explains, clearly and unambiguously, how the contract of sale will be concluded and how input errors can be corrected.

There are other detailed provisions that may impact on particular email marketing campaigns, and, as with all other Regulations and laws referred to here, advice should be taken in each case from the DMA Legal Department or other legal advisers.

#### ***v. Privacy and Electronic Communications (EC Directive) Regulations 2003***

Of all the regulations referred to here, these impose the most detailed obligations on email marketers.

They apply to all “transmission of unsolicited communications by electronic mail to individual subscribers”.

Detailed advice should be taken on the applicability of the Regulations in each case; but in summary, taking into account the various definitions in the Regulations, they impose the following obligations on all UK Data Users sending direct marketing email:

- to clearly state the identity of the Data User and
- to provide a valid address to which individuals can send an unsubscribe request.

The other email marketing restrictions in the Regulations apply only to Unsolicited Commercial Email Messages sent to “individual subscribers”, in



other words individuals receiving emails at a terminal where they are personally paying the relevant telephone bill or where the paying party is a partnership or sole trader (and not where the bill is being paid by a limited company or plc).

In these cases, the effect of the Regulations is as follows:

- except in “soft opt-in” situations (see next bullet point) no person shall transmit or instigate the transmission of an email unless the recipient has “previously notified the sender that he consents for the time being to such communications being sent, by or at the instigation of the sender for direct marketing purposes” (i.e. opted in) and;
- in a soft opt in scenario, the recipient does not need to have opted in to receiving the email before it is sent. However, four requirements must be met:
  - a. the sender or instigator of the sending (“**Sender**”) has obtained the recipient’s email address in the course of a sale or negotiations for the sale of a product or service to that recipient;
  - b. the email is in respect of the Sender’s "similar" products or services;
  - c. the recipient has been given a simple means, without charge, (other than the cost of the means of transmission used) of refusing the use of his email address for email marketing, both at the time when the email address was first captured and in each subsequent communication, and has not done so; and
  - d. the Sender of the email has clearly stated its identity.

## ***vi. The CAP Code***

Paragraph 43.4 requires that

"The explicit consent of consumers is required before:

...

sending marketing communications by e-mail..., save that marketers may send unsolicited marketing about their similar products to those whose details they have obtained in the course of, or in negotiations for, a sale. They should, however, tell them they can opt-out of future marketing both when they collect the data and on each occasion they send out marketing and should give them a simple means to do so. Explicit consent is not required when marketing business products to corporate subscribers (see 1.3j), including to their named employees."

Clause 1.3j states that:



"a *corporate subscriber* includes corporate bodies such as limited companies in the UK, limited liability partnerships in England, Wales and N. Ireland or any partnerships in Scotland. It also includes schools, hospitals, Government departments or agencies and other public bodies. It does not include sole traders or non-limited liability partnerships in England, Wales and N. Ireland. See clause 43.4."

Marketers should note the difference between this rule and those contained in the 2003 Privacy and Electronic Communications (EC Directive) Regulations. The CAP Code only allows Unsolicited Commercial Emails to be sent to directors and employees of limited companies and plcs without consent if the emails are advertising goods and services, which such people would purchase in a business/professional capacity. The 2003 Regulations do not make this distinction and allow Unsolicited Commercial Emails to be sent to directors and employees of limited companies and plcs advertising goods and services which such people would purchase in a personal and a business /professional capacity.

## **vii. Bibliography**

1) Data Protection Act 1998

<http://www.legislation.hmsso.gov.uk/acts/acts1998/19980029.htm>

2) Privacy and Electronic Communications (EC Directive) Regulations 2003 can be accessed together with other information on the regulations via

[http://www.dti.gov.uk/cii/regulatory/telecomms/telecommsregulations/comms\\_dpd.shtml](http://www.dti.gov.uk/cii/regulatory/telecomms/telecommsregulations/comms_dpd.shtml)

Information Commissioner's Office Guidance to the Privacy and Electronic Communications (EC Directive) Regulations 2003 can be accessed via

<http://www.informationcommissioner.gov.uk/eventual.aspx?id=96>

3) The Electronic Commerce (EU Directive) Regulations 2002 covering transparency of electronic commercial communications can be accessed on

<http://www.legislation.hmsso.gov.uk/si/si2002/20022013.htm>

Further information can be accessed on the DTI site on

[http://www.dti.gov.uk/cii/ecommerce/europeanpolicy/ecommerce\\_directive.shtml#the\\_regs](http://www.dti.gov.uk/cii/ecommerce/europeanpolicy/ecommerce_directive.shtml#the_regs)

4) The Consumer Protection (Distance Selling) Regulations 2000 covers sales at a distance including mail order, the Internet or by telephone. Access the Regulations on

<http://www.legislation.hmsso.gov.uk/si/si2000/20002334.htm>



and further information can be found on

<http://www.dti.gov.uk/ccp/topics1/guide/distsell.htm>

The 2000 Regulations do not cover distance sales of financial services, which are covered by a separate EU Directive, due to be implemented across Europe by October 2004.

5) The CAP Code can be accessed via

[www.cap.org.uk](http://www.cap.org.uk)

6) Information Commissioner's Office website is at

[www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk)

## **APPENDIX B. Insights into Deliverability**

Deliverability refers to the issues surrounding the delivery of an email campaign to the targeted individuals.

As a result of an increase in 'spam' by 'spammers' operating outside an accepted framework, ISPs have taken steps to protect their customers; companies to protect their employees; parents to protect their children; and individuals to protect their inboxes – using a variety of different technologies and solutions to block unwanted email. This section looks at what can happen to a marketing email on its path to an individual.

### ***i. Individuals controlling delivery***

There are two main ways for individuals to control the amount of email they receive. The first of these are through the user settings on their email client. The second method involves the installation of filtering software locally on their machines. This filtering software is readily available on the internet and has varying degrees of effectiveness in combating the email problem at the consumer level.

### ***ii. ISP Blocking/Filtering***

The technology employed by ISPs differs widely in its sophistication. Here are some of the methods used:

#### ***Volume based blocking and filtering***

The ISP makes deliverability decisions based on the amount of email sent from a single source.

#### ***Content based blocking and filtering***

The ISP accepts the email but scans the content and uses a scoring technique to identify if the email is a piece of spam. The scoring again differs widely across ISPs.

#### ***Image content based blocking and filtering***

This is based on the ISP's ability to identify flesh tones in the graphics.

#### ***Reply-Confirm, also known as Challenge/Response***

When an email is received from any given address for the first time, the ISP holds this email in limbo and automatically replies to the sender with a random image. The sender must then reply with an answer to a question about that image. If the sender replies with the right answer the email is delivered. Otherwise it is deleted.

### ***iii. ISP user settings***

There are many settings available to subscribers at the ISP level to restrict what they actually receive. e.g.:

- using an age setting to restrict certain emails;
- restricting received emails to only those from addresses within the individual's address book; and
- a "This is spam" button.

While not a filter, the "This is spam" button, allows individuals to provide feedback to their ISP on what they perceive as spam instead of unsubscribing directly with the sender. In addition to this new button, some ISPs have started encouraging their customers to NOT use the unsubscribe functionality included in the email as some illegitimate 'spammers' use this as a tool to validate email addresses.

The challenge here for responsible marketers is that ISPs will block email which has received too many of the "This is spam" complaints, so while it may be a legitimate opted in email, a disgruntled customer(s) can prevent others from receiving legitimate opt-in emails

### ***v. Corporates controlling delivery***

Most corporate bodies use firewalls to protect their data and infrastructure from internal and external abuse. Many of the techniques described above will be replicated by a firewall or other software packages added on to the corporate mail server. In addition to these, a standard firewall setting can simply reject all HTML emails. Also because of the ease with which they are implemented, many corporate postmasters use real-time black lists to help block spam.

### ***vi. Filtering Software***

Software products available to individuals to use at home will give greater control to the individual on the type of emails they receive, but in turn may prevent them from receiving email from a legitimate source, regardless of whether they have positively opted in.

In similar ways to technology employed by ISPs, the software will scan and build scores on key words and/or image content. Some products also include in the scoring the number of links (URL's) being used in the email. Direct Marketers have always worked on the basis of providing as many opportunities as possible to respond, but software using link numbers as a means of identifying spam may preclude a legitimate email marketing communication being delivered.



### ***vii. Real-time Black Lists (RBLs)***

Real-time black lists (RBLs) are also being used to reduce unwanted emails.

These lists block emails on behalf of their clients from any domain they deem to be delivering spam. This is accomplished by routing all inbound mail traffic through the RBL before delivering it to the mail server, which is how they are able to add and delete IP addresses from their list in real time.

The RBLs all have different rules for offending IP addresses but as a general rule they measure the volume of emails delivered vs. the number of complaints.

RBLs are frequently used by smaller ISPs that lack the resource to employ a sophisticated system for combating unsolicited email.



## **APPENDIX C. Glossary**

### **Above-the-fold**

The part of an email or web page that is visible without scrolling.

### **Appending Data**

Amalgamating data about an individual from multiple sources.

### **Auto Preview**

The view email software provides an individual to see without fully opening the message.

### **Blocking**

Emails that are blocked are not processed through the ISP or firewall and are essentially prevented from reaching their addressed destination.

### **Cell Testing**

When the list is divided into a number of discrete cells to allow for a robust test across multiple variables. To determine optimum response, response rates are measured for each cell.

### **Challenge/Response (Reply/Confirm)**

When an email is received from any given address for the first time, the ISP holds this email in limbo and automatically replies to the sender with a random image. The sender must then reply with an answer to a question about that image. If the sender replies with the right answer the email is delivered. Otherwise it is deleted.

### **Click-Through Rate (CTR):**

The number of people per 100 (expressed in percentage terms) who click through to a URL embedded in an email, banner ad, text or graphic, to view a specific web page. Click-through rates can be reported against the total number of click-throughs (allowing multiple click-throughs from one IP address), or against the number of unique users who click through.

### **Consent**

Any freely given specific and informed indication of an individual's wishes by which the individual signifies their agreement.

## **Conversion Rate**

The key metric to evaluate the effectiveness of a conversion (often sales) effort, reflecting the percentage of people converted into buyers (or whatever action is desired) out of the total population exposed to the conversion effort. For websites, the conversion rate is the number of visitors who took the desired action divided by the total number of visitors in a given time period (typically, per month). For email marketing, the conversion rate is the percentage of people who take an action out of the total number of people who received the email.

## **Cookies**

A "cookie" is a small piece of information that a web server can store temporarily with a web browser. This is useful for having a browser remember some specific information that the web server can later retrieve.

The main purpose of cookies is to identify users and possibly prepare customised web pages for them. An individual entering a web site using cookies may be asked to fill out a form providing such information as their name and interests. This information is packaged into a cookie and sent to the individual's web browser that stores it for later use. The next time the same web site is visited, the browser will send the cookie to the web server. The server can use this information to present the individual with custom web pages. So, for example, instead of seeing just a generic welcome page a welcome page with the individual's name on it is seen.

## **CPA (or Cost Per Acquisition)**

A payment model in which payment is based solely on qualifying actions such as sales or registrations.

## **CPM (or Cost Per Thousand)**

In email marketing, CPM commonly refers to the cost per 1000 names on a given rental list.

## **CPR (or Cost Per Response)**

This term is used to track responses, where the desired result is not purchase, click-through or cost per number of emails for the campaign).

## **CRM (or Customer Relationship Management)**

This describes a strategy and execution, not just from a marketing perspective, for managing the whole of the Data User's relationship with its customers.



## **Data**

Information which:

- is processed, or is recorded with the intention that it should be processed, by means of equipment operating automatically in response to instructions given for any direct marketing purposes, however it is accessed and whether or not it is in the form of a list
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system (i.e. manual data where data is structured in such a way that specific information relating to a particular individual is readily accessible).

## **Data Controller**

A person or organisation that, either alone or jointly, determines the purposes for which, and the manner in which, any personal data are, or are to be, processed.

## **Data Processing**

Collecting or storing information or data; or carrying out any operation/s on the information or data.

## **Data Processor**

A person who collects, stores or deals with personal data on behalf of a data controller (including a list broker/manager).

## **Data User**

An organisation making use of either its own data or of data obtained from other sources for any direct marketing purpose.

## **Data Subject**

An individual who is the subject of personal data.

## **Data Supplier**

A data controller who makes data available to third parties for use in their direct marketing activities.

## **Distribution (Gross)**

The total number of emails sent as part of a single campaign/distribution to all (SMTP) addresses on the distribution list.

## **Distribution (Net)**

The total number of emails successfully sent as part of a single campaign/distribution to all (SMTP) addresses on the distribution list.

## **Dynamic Content**

Variable content within an email message, including images and text, that is displayed in an email based upon information held in a database.

## **Duplication**

Multiple entries in any database of the same individual.

## **Email Marketing**

Direct marketing using email as a delivery method. For the purposes of these Guidelines, this specifically excludes SMS.

## **Email Preference Service**

A US DMA hosted register of individuals who have registered their wish not to receive unsolicited email messages.

## **ESP**

Email service provider.

## **Exclusion**

Soft Opt-In allowing email marketing communication without positive consent, subject to conditions.

## **GIF (Graphic Interchange Format)**

Graphics format most commonly used on web pages and in email marketing messages. They display 256 colours and have built in compression, which makes file size smaller, and load time quicker.

## **Harvesting**

The collection of email address directly from websites and the internet, without seeking consent for usage.

## **Hard Bounce/Soft Bounce**

A hard bounce is the failed delivery of an email due to a permanent reason like a non-existent address. A soft bounce is the failed delivery of an email due to a temporary issue, like a full mailbox or an unavailable server.



## **Headers**

The information that accompanies the body of an email message. Headers contain information on the email and the route it has taken across the internet. Some header information is visible to an individual in an inbox; other information is hidden as a default. It includes the "to" (identity of individual), "from" (identity of sender) and "subject" (information in the subject line).

## **House File**

A list that is primarily used and controlled by the Data User.

## **HTML (hypertext markup language):**

The language which gives a web browser specific instructions on how to display a formatted document in the browser window. HTML has a specific group of standards that makes it universal to all computer platforms.

## **HTML Email**

An HTML email is one that is graphically rich with colour and images and is emerging as the standard for email marketing. Marketers have to keep in mind that some recipients do not want to receive their emails in HTML, due to low bandwidth and/or the longer download times that HTML messages require at times. However, HTML messages often pull a higher response than plain-text messages.

## **Individual**

A living person to whom the Data User wishes to send a marketing email.

## **ISP (or Internet Service Provider)**

A company that connects users to the internet, sometimes referred to as an On-line Service Provider or Access Provider.

## **JPEG**

Another of the many graphics formats used in web and email design. A compressed format better used for photographic or continuous tone information.

## **Landing Page**

The page on a website where the visitor arrives (which may or may not be the home page). In terms of an email campaign, one can think of the landing page as the page to which the email directs the prospect via a link.



## **Legacy Data**

See House File.

## **Links**

Text links, hyperlinks, graphics or images which, when clicked or when pasted into the browser, direct the prospect to another online location. To be most effective in motivating action, links must be obvious to the visitor or recipient.

## **List**

A database of email addresses and all other personal data collected and held in connection with marketing and related purposes.

## **Load Time**

The length of time it takes for a page to open completely in the browser window.

## **Mailing List**

A set of email addresses designated for receiving specific email messages.

## **Multipart alternative email**

A multipart alternative email contains both a text and HTML version and will display the most appropriate version for the email client that it is sent to.

## **Navigation**

The tabs, text and graphic hyperlinks that always let individuals know both where they are and where they can go. Navigation elements must always be available and obvious. Well-designed navigation will lead the prospect in the intended direction.

## **Open Rate**

The percentage of emails opened in any given email marketing campaign, or the percentage opened of the total number of emails sent.

## **Opt-in (or Subscribe)**

Where an individual has positively indicated that he or she does not mind receiving unsolicited direct marketing email.



## **Opt-Out (or Unsubscribe) (of email marketing)**

Where an individual requests not to be included on an email list at the point of data collection or with subsequent communications. This is also referred to as unsubscribe.

## **Personal Data**

Information from which a living individual can be identified, whether from that information alone or combined with other information, which is in the possession of, or is likely to come into the possession of, the data controller. Members should be aware that information might be personal data even where an individual is not named, if it is possible to identify that person using information obtained from other sources. Business information and email addresses from which a living individual may be identified are also regarded as personal data and are covered by these rules.

## **Personalisation**

The practice of writing the email to make the recipient feel that it is more personal and was sent with him or her in mind. This might include using the recipient's name in the salutation or subject line, referring to previous purchases or correspondence, or offering recommendations based on previous buying patterns.

## **Privacy Policy**

A clear description of a website or Data User's policy on the use of information collected from and about website visitors and what they do, and do not do, with the data.

## **Privacy**

The quality or condition of being free from unsanctioned intrusion. Communications need to reassure the prospect through clear, accessible and enforced assurances so he/she can feel comfortable about providing personal information and transacting business.

## **Prospect**

A person who actively expresses interest in the product or service.

## **Rental list (or Acquisition list)**

A list of prospects or a targeted group of recipients who have opted-in to receive information about certain subjects.



## **Readability**

The degree to which the copy is well written as well as optimised for reading on the web. The readability of text is affected by many factors including, but not limited to: the colour of the text in relation to the background colour, the font, the spacing between words and between lines of text, the length of lines of text, how blocky and dense the paragraphs appear, text justification, the complexity of the grammar and the education level of your audience.

## **Segmentation**

Segmentation is the act of taking your email list and separating it so that recipients get different content based on their demographics, buying patterns, interest areas, etc.

## **Signature File (Sig File)**

A tagline or short block of text at the end of an email message that identifies the sender and provides additional information such as company name and contact information. Use it to convey a benefit and include a call-to-action with a link.

## **Soft Opt-in**

Where an individual is considered to have opted-in, on the basis that they have provided their email address during a sale or during the negotiation of a sale and other conditions are met, including that the individual was informed of how the information they provided would be used and were provided with an opportunity to opt out (see 2.1.1).

## **Solicited email**

Where an individual has actively invited the Data User to send the individual commercial email.

## **Spam**

Spam is the name given to random, untargeted bulk commercial e-mail where recipients did not request communications.

## **Subject Access Request**

Subject access request means a request made by an individual under S7 of the Data Protection Act 1998 regarding data about that individual being processed by the recipient of the request.

## **Subject Line**

The title of the email communication. This is the first element of the communication recipients will see when they access their email.



## **Subscribe**

See Opt-in.

## **Targeting**

Sending the right message to the right recipient at the right time.

## **Tracking**

Collecting and evaluating the statistics from which one can measure the effectiveness of an email or an email campaign.

## **Unsolicited Commercial Email**

Where an individual has not invited the Data User to send the specific message.

## **Unsubscribe**

Where an individual requests not to be included on an email list at the point of data collection or with subsequent communications. This is also referred to as opt-out.

