



# **Email Marketing Council**

## **Best Practice Guidelines**

June 2007

# Contents

Original Foreword to the 2004 Version .....	3
Acknowledgements .....	4
1.0 Introduction .....	5
2.0 Collecting and Managing Data .....	6
2.1 Data collection .....	6
2.2 Data hygiene .....	11
2.3 House Files. Data collected pre 2003.....	12
2.4 Renting Lists – ‘Host Mailing’ .....	13
2.5 Appending Data.....	15
3.0 Email Campaigns .....	17
3.1 Campaign Hints and Tips .....	17
3.3 Other Key Issues.....	23
4.0 Standard Metrics for Measurement and Reporting .....	26
4.1 Delivery Metrics.....	26
5.0 International Issues.....	28
5.1 Transferring data outside the EEA .....	28
5.2 Emails received outside the UK.....	29
6.0 Complaints and Dispute Resolution .....	30
APPENDIX A. Legal and other regulatory requirements.....	31
i. Summary .....	31
ii. Bibliography .....	32
APPENDIX B. Deliverability .....	34
APPENDIX C. Glossary .....	37



## **Original Foreword to the 2004 Version**

I welcome the DMA's initiative in putting together accessible guidance on all aspects of email marketing. I am pleased that appropriate prominence has been given to the requirements of the Privacy and Electronic Communications Regulations 2003 and to the steps that can be taken to reduce the prevalence of Spam.

Richard Thomas  
Information Commissioner



## Acknowledgements

Welcome to the new and revised DMA Email Marketing Best Practice Guidelines. I would like to take this opportunity to thank all those that have contributed to making this a comprehensive and informative document that will help marketers get the most out of what is an exciting and interactive marketing communication channel.

In particular, I would like to thank the members of the Best Practice and Legislation Hub of the DMA's Email Marketing Council:

- Steven Groom – Osborne Clark
- Simone Barratt – e-Dialog
- Fiona Cuthbert – Acxiom
- Sarah Collin – CACI
- Dela Quist – Alchemy Worx
- Liz Woodbridge – Mardev
- Omaid Hiwaizi – Crayon
- Simon Jeffs – TMN Media
- Jackie Clode – Dennis List Solutions
- Robert Dirskovski - DMA

### **Rupert Harrison**

News International

Chair of Legislation & Best Practice Hub, DMA Email Marketing Council



## 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 British Code of Advertising, Sales Promotion and Direct Marketing (the CAP Code). Nor are they advice on the relevant laws, most importantly the Data Protection Act 1998 ("the 1998 Act") and 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 and 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.

However just before going into detail it may be helpful to review the summary data glossary below:

Term	Definition
Data Subject	A living individual who is the subject of personal data.
Data Owner	An organisation responsible for the collection, storage and maintenance of the email data.
Data User	An organisation making use of either its own data or of data obtained from other sources for any direct marketing purpose.
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. (including a list broker/manager).
Data Processor	A person who collects, stores or deals with personal data on behalf of a data owner or data controller
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.

### 2.1 Data collection

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

- 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 necessary for the purpose for which the data will be used;
- have a clear Notice providing all requisite data protection notices and a link to, or full details of, a Privacy Policy at the point of data collection;
- comply with all relevant codes, including, but not limited to the DMA's Direct Marketing Code of Practice and the CAP Code;
- gain positive consent to send Unsolicited Commercial Email Messages (for example with the use of an 'Opt-In' tick box), unless the soft opt-in exception below applies (see 2.1.1 below):



- 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 on each subsequent marketing email, with reasonable prominence and that it is easy to use
- comply fully with the requirements below of 2.1.2 Data Protection Notices and 2.1.3 Privacy Policy.

Furthermore, Data Users should send a confirmation email after individuals have signed up to receive unsolicited commercial emails that a) clearly confirms what the person has signed up for and what data they have 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 highly likely to involve contravention of the 1998 Act and the 2003 Regulations.

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

The Soft Opt-In Exclusion can be used when all of the following conditions are met:

#### **1. Email address collected in the course of negotiations for the sale of or the sale of a product or service**

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 a sale or negotiations for the sale of a product or service to the prospect or customer.

#### **2. Consumer told e mail address would be used for marketing purposes and offered an unsubscribe facility**

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.



### **3. The marketing relates to similar products and services of the organisation which collected the data**

"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 (see Appendix A and Bibliography), however, on how these phrases should be interpreted.

Best Practice is adhering to the ICO's interpretation as follows: 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 start. However, the ICO 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 and has been informed that cookie technology is being used (See section 2.1.2). 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 grocery supermarket) would expect at some point in the future to receive further emails promoting the diverse range of goods available at the supermarket, but not products such as car insurance. It is not permissible to send email marketing about a diverse range of products and services available from the company unless the individuals could be deemed to know about such a range. It is not permissible to send email marketing from other companies within the same company group. In the example given above, the car insurance would normally be sold by a separate company to the supermarket within the same group. In both situations the Data User would need positive consent as the soft opt-in exclusion does not apply in these situations.

### **4. The identity of the sender not disguised**

#### **2.1.2 Data Protection Notices**

When collecting an email address (online or offline), a data protection notice (see 2.1.3 below) must be prominently displayed (as a 'notice') at the point of collection:

When drafting a Data Protection Notice, the following points need to be noted:



- The notice must 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). It must also include the following, unless this information is provided elsewhere on the website: company registration number, country of company registration, Vat number and any membership of a trade/professional association.

The notice must provide clear and unambiguous details of the purpose or purposes for which the email address (and any other personal data being collected) is to be used. In particular, 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.

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 the individual must be 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. If you wish to share the email address with other limited companies within the same group as that of the Data User, then the following requirements must be met. If so the relevant company names must be given and the postal addresses should also be provided in addition to the company registration number, country of company registration, VAT Number and any membership of a trade/professional association should also be given in respect of each of the group companies, unless provided elsewhere on the website. In addition a description of the group companies 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 must 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; (NB The soft opt-in exclusion cannot be used in these circumstances).
- 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 together 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 must make as a matter of law and should make as a matter of 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". However, this is on the strict 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.

Whether data is collected in an online or offline environment, a Data Protection Notice must always be given at point of data collection, further to and irrespective of the provision of any Privacy Policy.

Data Users will need to take care to ensure that their Privacy Policy is tailored to their particular needs and the expectations of their prospects and customers are 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 email address use.



Please refer to section 19.22 of the DMA Direct Marketing Code of Practice for further information.

Data Users will need to take guidance and/or independent legal advice on the terms of their own particular Privacy Policy.

## **2.2 Data hygiene**

Data Users should ensure that they capture and store the data load date and the source from which the data was obtained. The latter is particularly important if the data user obtains information from multiple sources.

Good list hygiene practices, ensuring the quality of customer and prospect data, are critical to developing consumer trust and also helping 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; 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 hygiene 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 a maximum of 10 working days, but in any case Data Users must avoid sending further email marketing to individuals who have unsubscribed,
- to inform those unsubscribing that their request has been received and 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 opts back-in/re-subscribes, 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. Data collected pre 2003**

### **2.3.1 Existing personal data**

In order to assess a house file which includes email addresses in existence before 11 December 2003 (when the 2003 Regulations came into force), Data Users must segment these as follows:

- i. Customers and prospects that have provided positive consent to the receipt of email marketing by the Data Controller and have not subsequently unsubscribed.
- ii. Existing customers from 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 emails 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 email'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, together with a copy of the wording or telephone script used. In all such cases, positive consent must be obtained.

### **2.3.2 New personal data**

When collecting new personal data for House Files, reference should be made to the "Data Collection" section at 2.1 earlier in these Guidelines.

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

There are several ways that a Data Owner or Controller may rent out an email address 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 Owner or Processor 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 Owner must have obtained the positive consent of individuals to send such ‘host mailings’ (the Data Owner cannot rely on the Soft Opt-in Exclusion for this type of marketing);
- the Data Owner’s email database is not passed to the Data User other than for de-duplication processes (however also see 2.4.1)
  - Often, the Data Owner or Processor will supply the corresponding postal address file to the Data User, who will carry out a dedupe/match and simply supply back the URNs of the records required for broadcast
- the Data Owner’s name must appear in the ‘From’ box of the email as the sender of the email; and
- the Data Owner or Processor must manage the unsubscribe process as described under ‘Data Hygiene’.

It is the responsibility of the Data User to be satisfied as to the circumstances in which the email addresses came into the possession of the Data Owner. It is advisable to have a written agreement in place.

Amongst the areas of enquiry the Data User should pursue with the Data Owner or Processor 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 and 2.1.3) Further to an adjudication by the Advertising Standards Authority, it is now highly advisable for the Data User to ask to see a written copy of the Data Protection Notice to satisfy itself that appropriate consents have been obtained. It is not enough to merely accept an assurance (written or otherwise) that consent has been obtained<sup>1</sup>;

---

<sup>1</sup> Advertising Standards Authority Non-broadcast adjudication Home Entertainment Corporation plct/amoviechoices.com 13 October 2004  
[http://www.asa.org.uk/asa/adjudications/non\\_broadcast/Adjudication+Details.htm?Adjudication\\_id=38716](http://www.asa.org.uk/asa/adjudications/non_broadcast/Adjudication+Details.htm?Adjudication_id=38716)



- 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 Owner or Processor has been otherwise legally compliant as regards the collection and subsequent use of the email addresses.

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

#### **2.4.1 Host mailings and using a different ESP to deliver the email**

As part of the host mailing service offered by Data Owners for acquisition campaigns Data Owners may have in place a broadcast solution with an ESP (Email Service Provider).

The cost of transmission may be included in the CPM (cost per thousand) or it may be an additional charge.

In some cases it may be preferable for the Data User to have a different ESP to undertake the transmission or broadcast of the mailing. The reasons for this might include; for de-duplication purposes (against house or customer file and other cold lists), so that the Data User can track the campaign on their designated ESP as they are familiar with their reporting suite or simply because they want to have complete control of the timing.

Best practice allows a different ESP to deliver the email so long as certain criteria are met:

1. There is a non-disclosure agreement in place between the Data User or Processor and the Data Owner.
2. The Data Owner's header and footer template is used.
3. the Data Owner's name must appear in the 'From' box of the email as the sender of the email;
4. The designated ESP is able to provide the unsubscribes from the campaign back to the Data Owner or Processor within 48 hours. This is essential for list hygiene.

## **2.5 Appending Data**

### **2.5 Appending information**

Appending is the process of attaching additional information to your customer records. In the email-marketing world this could either be:

- Attaching demographic or lifestyle data to your email record (assuming you have a name and address data as the match key) or
- Attaching an email address to an existing customer name and address record.

In the first instance, attaching additional information to an email record would be the same as attaching demographic and lifestyle data to any other name and address record but in this case, you happen to have their email address as well. This is common practice for marketers and is legal as long as such appending is in compliance with the 1998 Data Protection Act and the Privacy and Electronic Communications Regulations 2003.

The second case is more complex and all hinges around the permissions, which have been given. Appending email addresses is permitted when the individual has given third party permission to a data owner which makes it clear at the time of opt-in that their data may be shared with third parties.

Appending will also be permitted when an individual has explicitly opted-in to receive email marketing messages from a particular company, via an email from the original data owner. If this permission has been given then an email address can be appended.

Having consented to their email address being shared in this way, it is then best practice for the individual to be sent a message either from:

- a) The Data Owner to explain that their email address will be passed onto the client company and provide them with an initial opportunity to opt-out from this happening or
- b) The client company who will be the recipient of the email address to explain to the individual where they got their email address from and giving them the opportunity to refuse further emails from them.

Appending in the business-to-business area should be done in the same manner where only an individual who has given consent to receive unsolicited marketing material should be contacted. It is not best practice to use predictive techniques to work out other individuals email addresses at an organisation – indeed; in some cases it is illegal.

The key areas that the data user needs to satisfy before undertaking an email appending exercise are as follows:

- How and when the list was built. If the list is an amalgamation of different suppliers' data you would need to be satisfied about what data



protection notices and privacy policies were in place at the point of data collection by each supplier.

- How unsubscribe requests have been processed and relevant addresses suppressed.
- That the data user is covered by a data licence, which ensures they comply with the 1998 Data Protection Act and the Privacy and Electronic Communications Regulations 2003.

Best practice may suggest that only customer data is appended, as the individual would already be familiar with the data user.

That the individual is informed of what is happening to their data, understands where the original consent comes from, can see a privacy statement of the data user and has an opportunity to refuse before any data is passed to the data user.

That the individual can easily opt-out/unsubscribe from the data owners list.

## 3.0 Email Campaigns

There are many factors that can determine the success of an email campaign – indeed there are many ways to define the success of a campaign. And as each campaign is conceived, clear goals should be established – and then tracking put in place to capture data that will inform the campaign manager to what degree those goals have been achieved.

Simplistically the focus should be on getting:

*‘the right message to the right person at the right time’*

More specifically this intent can be broken down:

<i>‘the right message . . . ‘</i>	<ul style="list-style-type: none"> <li>- is it the right offer?</li> <li>- is it the right product?</li> <li>- is it the right incentive?</li> <li>- is the tone appropriate?</li> <li>- is the creative/visual appropriate?</li> <li>- is it the right call to action?</li> <li>- is the email format appropriate?</li> </ul>
<i>‘ . . .the right person . . . ‘</i>	<ul style="list-style-type: none"> <li>- is it going to the right segment?</li> <li>- how can you personalise the message?</li> </ul>
<i>‘ . . . at the right time’</i>	<ul style="list-style-type: none"> <li>- is it being sent at an appropriate time -             <ul style="list-style-type: none"> <li>o customer buying cycle?,</li> <li>o time of year, month, week?</li> <li>o event associated - based on interest expressed or inferred?</li> </ul> </li> </ul>

### 3.1 Campaign Hints and Tips

#### 3.1.1 Personalisation and 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 and the use to which the data will be put, bearing in mind that any data must be relevant, adequate and not excessive to the Data User's needs.

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. At all times data is captured the individual must be told of such data capture and given the opportunity to object. If capture is via the use of a cookie the technology must be explained to the individual and he or she must be given the opportunity to object before any such technology is downloaded onto their computer.

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

### 3.1.2 Targeting

Targeting is an essential requirement of any marketing activity. Reaching the correct audience with the correct offer is the primary objective.

You can either create segments in your data to which different emails are created and sent. Or you can use 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.

### 3.1.3 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 although Outlook does translate plain text links automatically. Plain text is typically found within early versions of Lotus Notes and can be set by individuals as a preference in most email clients.

### 3.1.4 Rich text emails

Rich text emails are an evolution of plain text. These software packages allow for both coloured and variable fonts. In addition, rich text also supports hyperlinks. By clicking on a URL the internet browser on the computer is launched which takes the individual directly to the web site. Almost all versions of email reader accept Rich text – it is down to whether the email is sent as such, and the user has the option to receive such email turned on.

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.

### **3.1.5 How do I know what Email Format my Customers can receive?**

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 (typically those who read their emails offline) may prefer a text email as opposed to an HTML email.

Secondly, most 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.

HTML emails can also include **rich media** (e.g. flash animations and/or streaming video). Such content is either sent as an embedded file or linked to a hosted file. In either case, such content can be blocked by corporate firewalls and is not viewable in all email readers and hence it is very difficult to guarantee that all recipients will be able to see the animation or video.

### **3.1.6 The Design/Structure/Layout of the Email**

The layout of an email is as important as any other communication. Usually, an email appears in portrait requiring the recipient to browse down the page. Research has 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 –

- Creative and design should take into account restrictions imposed by HTML coding. A design that cannot be coded is counterproductive.
- Wherever possible use a template to gain production efficiencies and aid customer navigation as they become familiar with the layout over time.
- 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.

### **3.1.7 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 can mean one of several things:

- A) When the email reader is set to ‘auto preview’, the first paragraph of the plain text version of the body copy is visible for each email in the inbox.
- B) When the email reader is set to display a ‘reading pane’ at the bottom of the screen, the first 100-200 pixels (depending on screen resolution and the user’s preference for the size of the reading pane) from the top of the email are displayed when that email is selected.
- C) When the email reader is set to display a ‘reading pane’ at the right of the screen, then the first 200-300 pixels (again depending on screen resolution and the user’s preference for the size of the reading pane) from the left of the email are displayed when that email is selected.
- D) In any case, when the email is opened full screen in either an email reader or a web browser (in the case of web mail), then whatever portion of the email is visible without scrolling (typically the top 500 pixels on a 1024x768 screen).

It is generally accepted that the 3 second rule applies to email, so the most compelling copy or image should appear here to encourage the individual to open the email and read on.

As image blocking becomes increasingly prevalent alt tags should be included in the creative and design thinking. This is also required for accessibility.

A hosted version of each email should be included as a link in both HTML and text versions of all emails. This will ensure as many people as possible have access to the HTML version.

Links to the hosted version of emails can generated as much as 5% of the total clicks for that campaign.

### **3.1.8 The Size of the Email**

Given the differences in access to the internet, it is sensible to keep emails small to keep download times to a minimum. Despite the increasing prevalence of Broadband it is still a good idea to keep the weight of your HTML emails down as large messages are more likely to get caught in Spam filters. As a guideline messages should not exceed the 60k in total file size.

To reduce the size of the email, various techniques can be employed including not embedding images but serving them from an image server. Large images whether served or embedded can also cause emails to be caught by Spam filters if the message in the HTML has a low word count. Single offer mailings are more likely to suffer this problem than newsletters.



### **3.1.9 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 you send unsolicited commercial communications, for example, an email advertising your goods or services that is sent to a recipient who has not requested it, you must ensure that recipients are able to identify the email as such as soon as they receive it, either through looking at the subject line header or through wording in the body copy text.

If the email forms part of a regular communication, consider a consistent subject line such as “DMA Weekly Bulletin | 12.02.07”. 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. This is called split stream testing.

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 the content of your subject line. Be aware that not all words that trigger Spam filters are as obvious as “hot” or “free”, seemingly innocuous words such as ‘tips’, ‘enter’, ‘sample’, ‘private’, ‘reserved’, ‘products’ and ‘introductory’ could be viewed by filters as “spammy”.

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

## **3.2 Pre Deployment Testing (QA)**

### **HTML Rendering**

All email clients render HTML slightly differently which makes it difficult to guarantee a uniform customer experience. The fact a message looks great in Outlook does not mean it will look the same in AOL.

It is advisable to create a test list which should include an AOL account, Outlook and Outlook Express as well as the top 10 email domains or ISP’s (Yahoo, Gmail, Hotmail, ntlworld, Tiscali etc) on your list.

Prior to deployment, emails should first be sent to the test list and a visual check should be made in each account to ensure the HTML has properly rendered.



### 3.2.1 Frequency of Communication

Consider frequency of communication as a vital issue for recipients, as this 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 and possibly the length of the re-purchasing life-cycle of your product range. A newspaper publisher may deliver a daily email, whilst a retailer may deliver a weekly or monthly promotion.

Best practice would be to a) clearly inform people how frequently they will receive emails from you at the point of opt-in; and b) give them the option to choose the frequency rate.

A key metric that you should monitor is your opt-out rate. If your opt-out rate is on the increase, the frequency of your emails may be a factor. It would be worth considering a frequency test, or a survey to ask people's opinion. However, such a survey must not be sent to those individuals who have opted-out of receiving your email marketing.

### 3.2.2 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” or “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. Please see Section 5 of the DMA Direct Marketing Code of Practice, Data for further information.

### **3.3 Other Key Issues**

#### **3.3.1 Unsubscribe Process**

If the soft opt-in exception is being used the recipient must be given a simple means of refusing (free of charge except for the cost of transmission) the use of their contact details for marketing purposes at the time those details are initially collected and where they did not refuse the use of those details, at the time of each subsequent communication.

Therefore, one or more of the following methods for unsubscribing must be provided on every email:

- 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

#### **3.3.2 From Header and Subject Line - Transparency**

The Data User (or Data Processor 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'.

Please see Section 2.1.1, point 4 and 3.1.9 above for further information.

#### **3.3.3 Email Footer**

Following The Companies (Registrar, Languages and Trading Disclosures) Regulations 2006, every email marketing message should now include the company registration number, country of registration and registered office address.



### **3.3.4 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. Please refer to the Information Commissioner's Office who has published guidance – see Appendix A for details.

Marketers will need to obtain guidance from the DMA Legal Department or their legal advisers on a case-by-case basis.

### **3.3.5 Privacy Policy. Use of Cookies and Web Beacons**

In every email you must include:

- a clear link to the privacy policy of the Data Owner; and
- a clear link and comprehensive information on the cookie policy of the Data Owner where clear and comprehensive information about any cookie, clear gif, web beacon 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.

Best practice would be to rename the Privacy Policy link as “Privacy Policy and Use of Cookies” in order to raise the visibility of the use of cookies.

### **3.3.6 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 any age from under 12 years to less than 18 years.

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 without parent or guardian intervention there is no way to guarantee the age of any child who signs up for email marketing.

Given the extreme sensitivity of marketing to children, brands must take into consideration public perception and the potential brand damage of such



activity. Please see paragraphs 8.11 to 8.23 and 19.25 to 19.34 of the DMA Direct Marketing Code of Practice for further details.

### **3.3.7 Host Mailings – Working with suppliers of Data**

The section below addresses the relationship between a Data User and Data Owner 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 supplier of the Data:

*i. Written approval/ confirmation process:*

- Insertion Order (IO) to include some or all of 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 Owner or Processor 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 Owner, 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.

It is a legal requirement to have a data processor agreement in place. Guidance on such agreements can be sought from the DMA's Legal Department.



## 4.0 Standard Metrics for Measurement and 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.

As email marketing becomes more sophisticated it is also useful to look at customer orientated or behavioural metrics such as reach and frequency that are common currency in the offline world. Where such monitoring takes place and the data is to be processed on an individual basis, you must seek the individuals consent. However, where the data is to be anonymous such consent is not required.

### 4.1 Delivery Metrics

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

#### 4.1.1 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.

#### 4.1.2 Click Through Rate

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

#### 4.1.3 Click Through Metrics

- Gross Click Rate (Total Clicks/Total Delivered)
- Unique Click Rate (Unique Clicks/Total Delivered)
- Click to Open Rate (Unique Clicks/ Total Opened)

#### 4.1.4 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.



It is considered to be best practice to always pre-define measurement and success criteria and to track conversions accordingly. This can either be achieved directly using tracking technologies embedded with the email, or via a data match back process post campaign.

#### **4.1.5 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.

#### **4.1.6 Reach**

Data users can calculate the reach of their email marketing campaigns over time by calculating the number of unique openers or clickers over the period in question, e.g. 75% of the list opened at least one mailing in the last quarter.

#### **4.1.7 Frequency**

Data users can calculate frequency by working out how many issues each subscriber opened or clicked on, e.g. 22% of subscribers opened all 3 issues this quarter or 35% did not open any issues this quarter.



## 5.0 International Issues

### 5.1 Transferring data outside the EEA

The "Data Collection" section 2.1 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 27 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 guidance from the DMA Legal Department or your own advisor on the position while 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 Harbour" 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 Harbour 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 appropriate technical and organisational measures are taken to secure the data from physical theft or hackers. At all times the Data User is responsible for the actions of any Data Processor it employs and appropriate legal agreements, including a data processing agreement, must be put in place.

## **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 have transposed 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 guidance from the DMA Legal Department, other legal advisers and/ or consult the Information Commissioner's Office, as each country may operate slightly different regulations.



## 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 must be dealt with 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 must respect individual's rights under the 1998 Act 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 1998 Act 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 adjudicate on the matter.

## APPENDIX A. Legal and other regulatory requirements

### *i. Summary*

Best Practice in email marketing requires, as a minimum, compliance with UK legal and regulatory obligations.

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 as amended by the Consumer Protection (Distance Selling) (Amendment) Regulations 2005
- (c) specific rules applicable to email marketing in the Electronic Commerce (EC Directive) Regulations 2002;
- (d) specific rules applying to email marketing in the Privacy and Electronic Communications (EC Directive) Regulations 2003. In this connection practitioners are strongly advised to consult the DMA's summary of these Regulations and the "Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003 for Marketers published by the Information Commissioner's Office in December 2006;
- (e) the requirements for email marketing in the British 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 Direct Marketing 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 equivalent in the UK; and
- (j) the Communications Act 2003 and in particular its provisions prohibiting "persistent misuse" of electronic communications networks. and the Ofcom Statement of policy on the persistent misuse of an electronic communications network or service dated 1 March 2006.

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, independent advice should always be taken to ensure compliance.



## ***ii. Bibliography***

1) Data Protection Act 1998

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

Information Commissioner's Office Guidance to the Privacy and Electronic Communications (EC Directive) Regulations 2003 for Marketers dated December 2006 can be accessed via

[http://www.ico.gov.uk/upload/documents/library/privacy\\_and\\_electronic/detailed\\_specialist\\_guides/pecr\\_guidance\\_for\\_marketers\\_dec06.pdf](http://www.ico.gov.uk/upload/documents/library/privacy_and_electronic/detailed_specialist_guides/pecr_guidance_for_marketers_dec06.pdf)

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

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

Further information can be accessed on the DTI site on

<http://www.dti.gov.uk/sectors/ictpolicy/ecommsdirective/page10133.html>

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.opsi.gov.uk/si/si2000/20002334.htm>

and further information can be found on

<http://www.offt.gov.uk/NR/rdonlyres/1E6F3C94-8BB0-4374-A65B-6281E030C3C9/0/oft698.pdf>

5) The Financial Services (Distance Marketing Regulations 2004 are available from

[http://www.opsi.gov.uk/si/si2004/uksi\\_20042095\\_en.pdf](http://www.opsi.gov.uk/si/si2004/uksi_20042095_en.pdf)



Further information is available from

[www.hm-treasury.gov.uk/Documents/Financial\\_Services/eu\\_financial\\_services/fin\\_eufs\\_dmd.cfm](http://www.hm-treasury.gov.uk/Documents/Financial_Services/eu_financial_services/fin_eufs_dmd.cfm)

5) The CAP Code can be accessed via

[http://www.cap.org.uk/cap/codes/cap\\_code/](http://www.cap.org.uk/cap/codes/cap_code/)

6) Information Commissioner's Office website is at

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

Organisations frequently change pages on their websites,

The above links were correct as at 12 June 2007

## **APPENDIX B. Deliverability**

Unlike marketers in other disciplines, email marketers have to worry about getting their messages to their intended recipients. So regardless of how much time you spend on getting the copy just right and the care you put into your creative, it is all wasted if your message is not delivered.

There are some in the email marketing community, however that argue that ISP/IEP blocking is systemic and more than just a few false positives. Everybody can see how a campaign or a mishandled list could cause a temporary block, but the fact that the bigger ESPs have been forced to hire whole departments to handle ISP/IEP relations is evidence to some that the ISPs/IEPs are taking things too far.

This argument may have some validity and it is important that the industry continues to work to build good relations with the ISPs and IEPs. All of this however, is not going to do the marketer any good when they are sending out that all important campaign. What it needs to know is how a block could affect the ROI on the campaign and whether the additional costs to remove the block are justified in this instance.

The volume of Spam is driving the ISPs to block emails. Currently 80% of email traffic is spam, so there is a legitimate financial reason for the ISPs to control the amount of spam traffic on their networks.

The challenge in effectively blocking Spam however stems from weaknesses in the fundamental design of the standard protocol used (SMTP), which makes it hard for ISPs to which emails are legitimate and which are not. Sender ID/Sender Policy Framework (SPF) and Domain keys are two technical solutions that allow ISPs to authenticate who the email is really from, but these do not provide any guarantee into the reputation of the sender. Reputation is at the core of the both the Sender Score Certified and Goodmail Certified Email programs.

Email marketers should follow basic data hygiene rules that will allow them to be included in the ISPs white lists and hopefully off real time black lists.

### **Increasing Deliverability**

So now that we have a better idea of how emails get blocked, we will look at ways to improve email deliverability. The techniques to improve deliverability can be grouped into three categories:

- Permission
- List Hygiene
- ISP relations



## Permission

Permission is the key to all deliverability. In the UK, the legal requirement is that you get the subscriber's permission by them taking a positive action, which is fully informed and freely given before sending an unsolicited commercial email. There are two exceptions to this rule:

1. Business to Business emails sent to staff of limited companies and public limited companies with content that relates to business products or services.
2. Business to Consumer emails sent to individuals when all the following conditions are met.
  - (i) email address collected in the course of negotiations for the sale of or the sale of a product or service
  - (ii) consumer told the email address would be used for marketing purposes and offered an unsubscribe facility (easy to use and free of charge other than the cost of transmission) at the time of data collection and on every subsequent message sent.
  - (iii) the marketing relates to similar products and services of the organisation which collected the data
  - (iv) the identity of the sender not disguised.

Staff of sole traders and partnerships should be treated as individuals above under Business to Consumer regardless of whether the marketing relates to consumer or business products.

Following guidelines on opt-in and opt-out are vital components of permission. See section 2.0 above – Collecting and Managing Data.

## List Hygiene

After opt-in/opt-out policies and practices, maintaining list hygiene is the most effective way to maintain high deliverability rates. In off-line direct marketing, the cost of producing and mailing each pack acts as a deterrent to over mailing campaigns. In email marketing however, the marginal cost of each additional email does not hold the same disincentive. The result is that list owners have become lazy in removing invalid email addresses.

There are many reasons for email addresses becoming invalid. The first source of invalid email addresses is poor data collection. This is especially troublesome when email addresses are collected through offline means such as using the contact centre, product registration cards, etc. Using a confirmation email helps validate addresses collected offline but only if the sender stops sending to addresses where the emails bounce.

## ISP and IEP Relations

Regardless of how carefully you collect your opt-in data, process unsubscribe requests, and maintain good list hygiene, you will occasionally find yourself



being blocked. It is at this point you may need to contact the abuse experts at the ISP. The first place to look for information is at the ISP website. Here you will frequently find an FAQ page which will give you an idea of the source of your block. This area will also frequently give you contact details if you need to speak with somebody.

When speaking to an abuse representative, you should have all of the information to hand that they will need to help you. This includes:

- Your privacy policy
- How you collect opt-ins
- The date and time when the block started (if possible)
- A copy of the message that caused the block
- The IP address or range that is being blocked

While it is not guaranteed, frequently just the fact that you called is enough to get your first block lifted. Spammers never call to get blocks lifted, so your willingness to call gives you and your brand some legitimacy. Getting the block lifted however, is not the only reason for the call. You should also try to establish why you were blocked in the first place, so you can take corrective action and ask for advice on how to prevent future blocks.

A quick count on the domains in your email list will tell you which ISPs are the most important to you. Depending on the impact that a block would have it may be worthwhile to proactively begin to build relationships with these ISPs. You can begin this with an introduction of yourself and your brand that explains what you are doing and how you collected your data. This is also a good time to ask for advice on how to prevent blocks.

## **The future**

Going forward there will be a number of technical advances as well as other third party reputation services entering the market. Email marketers will have to keep abreast of these developments if they want to continue to receive their high rates of delivery.

Please see the white paper “Email Deliverability: How We Got Here and What Marketer’s Should do About It”, published by the Deliverability Hub of the Email Marketing Council of the DMA – available at [www.dma.org.uk](http://www.dma.org.uk) for further information.



## **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 external 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.

### **Bounce - Hard/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.

### **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.

### **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 call to action (often sales), 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 user's 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.

## **CPC (Cost per Click)**

Rather than paying a cost per 1000 emails delivered, or a cost per response, some suppliers charge a sum for all the recipients that click through on a marketing message.

## **CPM/CPT (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 Owner**

An organisation responsible for the collection, storage and maintenance of the email data.

## **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.

### **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 sent and successfully delivered 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 based upon information held in a database.

### **Duplication**

Multiple entries in any database of the same individual.

### **European Economic Area (EEA)**

The 27 Member States of the EU plus Iceland, Lichtenstein and Norway.

### **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. This service is only required when sending such emails outside of the EEA to people who are ordinarily resident outside the EEA



## **ESP**

Email service provider.

## **Firewall**

A firewall is a method of stopping spam, unwanted content, viruses, etc from reaching a users inbox. Usually used in a corporate context, however personal firewalls are becoming more popular.

## **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.

## **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. 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 (Joint Photographic Experts Group)**

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 email**

A multipart 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 delivered.



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

Where an individual has positively indicated that he or she wants to receive email marketing.

## **Opt-Out (or 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 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 is not currently a customer, but is deemed to be in the correct target market for a product or service marketing campaign as has provided relevant consent.



## **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.

## **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 email where recipients did not request communications.

## **Subject Access Request**

A subject access request means a request made by an individual in writing under S7 of the Data Protection Act 1998.

## **Subject Line**

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



## **Subscribe**

See Opt-in.

## **Targeting**

See segmentation.

## **Text format (to complement html)**

This type of email provides for black text only and any links to a web site appears as a complete URL such as <http://www.dma.org.uk/DMA/default.asp>.

## **Tracking**

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

## **Unsolicited Commercial Email**

See Spam.

## **Unsubscribe**

Where an individual requests not to be included on an email list to which they had subscribed with subsequent communications. This is also referred to as opt-out.

## **URL**

A Uniform Resource Locator (URL or, less formally, Web address) is a sequence of characters conforming to a standardized format, used for referring to resources (such as documents and images on the Internet) by their location, which is usually shown in the address bar at the top of a browser.

## **Web Beacons**

A Web beacon is an object that is embedded in a Web page or email and is usually invisible to the user but allows checking that a user has viewed the page or email. Alternative names are Web bug, tracking bug, pixel tag, and clear gif.

