

CONFIDENTIAL

OpCo Policy Guidance

Vodafone

Malicious and Unsolicited Communications Policy

September 2004 V.1.

Table of Contents

1. About this document	5
1.1 Governance	5
1.2 Purpose	5
1.3 Contacts	5
2 Executive overview	6
2.1 Review and update current approaches	6
2.2 Review current policies	6
3 Mandatory requirements for malicious communications	8
3.1 About malicious communications	8
3.2 Customer Support	8
3.3 Police and law enforcement involvement	9
3.4 Contractual measures	9
3.5 Malicious voice calls	10
3.6 Other types of malicious communications	11
4 Mandatory requirements for bulk unsolicited communications (spam)	13
4.1 About spam	13
4.2 National regulatory support	14
4.3 Unsolicited SMS soliciting a premium rate response	14
4.4 Stamp out SMS spam by making it uneconomic	15
4.5 Adoption of calling party pays	16
4.6 Customer contracts	16
4.7 Interconnection / Interworking	17
4.8 SMS content and PRS provider agreements	17
4.9 Technical solutions	17
4.10 Group Marketing support	18
5 In summary	19
APPENDIX I - Vodafone Ireland case study	20
Procedures for dealing with nuisance calls/messages	20
Public position	21
Customer education	21
Customer terms and conditions	22
Customer care script	22
APPENDIX II - SHARK initiative	23
APPENDIX III – Contract clause template	24

Document Control

Version	Date	Editor	Remarks
0.9	24.08.04	Caroline Dewing	Signed off by Content Standards Working Group
1.0	06.09.04	Caroline Dewing	Issue to OpCo Content Standards, Fraud and Security, Customer Operations, Consumer Platforms Messaging Group

Approval

Version	Name and Role	Signature and Date
0.9	Working Group	
1.0	Tina Southall	

Abbreviations

Acronym	Meaning
CLI	Calling Line Identity
CSR	Corporate Social Responsibility
CSSG	Content Standards Steering Group
CSWG	Content Standards Working Group
GPC	Group Policy Committee chaired by Arun Sarin with representation from
GSMA	Global Mobile Operators Trade Association
IPCM	Internet Protocol Commercial Model
MNO	Mobile Network Operator
PRS	Premium Rate Services
SMS	Short Messaging Services

Terminology

	Meaning
Malicious communications	Person to person communications that harass or abuse, or are intended to harass or abuse the recipient. As well as voice calls this also includes SMS, emails and new forms of mobile communications. This is sometimes described as malicious personal communications to distinguish it from bulk unsolicited communications (spam).
Bulk unsolicited communications (spam)	Messages sent in large volumes typically for commercial gain. These may involve marketing or "advertising", whether legitimate or illegitimate or, in the case of mobile, may solicit a premium rate response. Alternatively, unsolicited communications may be malicious and sent to many rather than be directed to individuals.
Premium rate response	A premium rate voice call, premium SMS or other premium rate reply made by a Vodafone customer to an unsolicited message inviting a response. Part of the charge for this service is paid by Vodafone to an end company linked to the sender of the unsolicited message. The payment is often via a number of intervening communications providers.
Active malicious content	Executable code or applications such as viruses or "malware" which are designed to disrupt the functioning of a Vodafone customer's device or to defraud the customer by carrying out unauthorised transactions.

1. About this document

1.1 Governance

In 2002 the Group Policy Committee set up Content Standards Group to develop a series of Group wide mandatory policies and best practice guidelines to govern the provision of content and services available via the Vodafone network. Where appropriate these policies will have a particular priority to protect younger users from age-sensitive content and services.

The aim is to ensure best practice across the business and, as such, all OpCos will be subject to a regular audit on their implementation.

1.2 Purpose

The purpose of this document is to share the learnings from other OpCos which have already experienced negative publicity and complicated customer issues through the use of new messaging products and services.

This document provides best practice guidelines for Operating Companies for dealing with:

- Malicious communications
- Bulk unsolicited communications (spam)

Each Operating Company should review its existing procedures in light of these guidelines and adopt any additional procedures necessary to address new forms of communications including MMS, video messaging, video calling, etc., that are now, or soon to become, available.

1.3 Contacts

For more information and guidance on implementation please contact Jenny Jones or Emma Crook of Content Standards OpCo Engagement within Vodafone Consumer Marketing.

jenny.jones@vodafone.com

+ 44 20 7212 0477

emma.crook@vodafone.com

+ 44 20 7212 0201

2 Executive overview

2.1 Review and update current approaches

Vodafone Operating Companies already have internal processes for dealing with malicious voice calls. However, this does not necessarily include new forms of malicious communications.

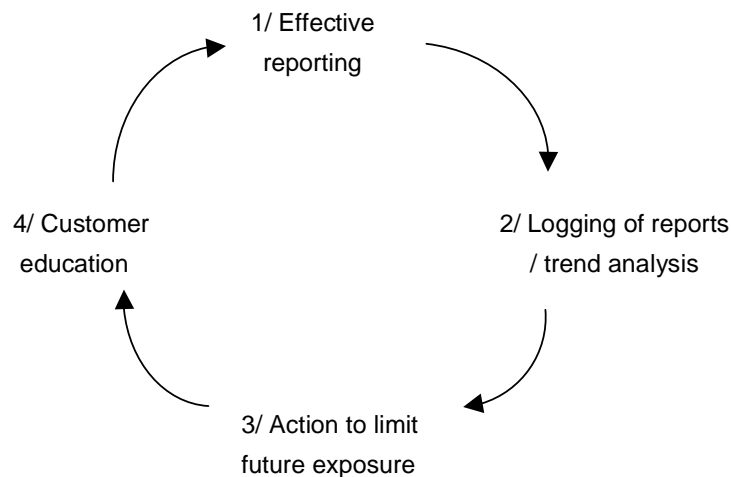
Currently, most Vodafone Operating Companies respond to customer concerns on malicious calls by attempting to stop it and reducing the likelihood of it happening again. In general, this includes:

- Offering advice on how to manage malicious calls
- Changing the customer number
- Liaising with national law enforcement agencies where malicious personal calls be particularly serious

Vodafone UK has taken steps to withhold out-payments made to premium rate services that were generated in response to spam messages. This has proved to be very effective and evidence suggests that the support of relevant regulatory authorities is vital in suppressing this form of spam.

2.2 Review current policies

It is a mandatory requirement that all Operating Companies review their current policies on spam and malicious communications. Revised malicious communications and bulk unsolicited communications policies should build on established procedures and include reference to new services and technologies, such as MMS, video messaging, video calling, IM etc., which are soon to be widely available. It should encompass both spam and personal malicious communications and should be based on the following 4-step approach: See details on following page.



-
- 1/Reporting** There should be a clear process for customers to report any type of malicious personal communications received by them or by another customer they are responsible for (e.g. a child) through Vodafone customer care.
- All procedures should be extended to services including SMS, MMS, video messaging, video calling etc., as these are made available.
- Vodafone Operating Companies should also provide a free-of-charge forwarding function to allow customers to report spam messages they receive - starting with unsolicited SMS soliciting a premium rate response. This should operate on an automated basis behind a short code (see 4.3).
- 2/Logging** All reports of malicious personal communications or bulk unsolicited communications should be logged to prioritise action and to identify intensity and trends.
- 3/Action** For malicious communications, Operating Companies should have a clear escalation process that includes defined Vodafone customer care responses in given circumstances. This should include processes for interaction with law enforcement.
- For bulk unsolicited communications, Vodafone should examine the kinds of messages forwarded to it. This will provide insight into the customers' experience with spam and this insight will determine the response. Where unsolicited messages are soliciting a premium rate response, Vodafone should use any suitable legal mechanism to withhold outpayments. This will suppress the economic incentive to originate such messages.
- 4/Education** Information for customers on how to respond to malicious personal communications, how to report these to Vodafone, and what we will do to support our customers, should be easily available. Customers should be informed that using our services for malicious communications or spam is unacceptable and the contract terms of service should reflect this by stating clearly that Vodafone may terminate its service to a customer who originates malicious communications or spam.

Together, these four steps will support effective action against malicious and unsolicited communications.

Even where Vodafone is not able to suppress these activities, it is important for our business to have an accurate idea of what customers experience. Understanding this will allow us to modify our services to increase the level of customer satisfaction. It will also allow us to develop and present an informed position regarding the potential regulation of new mobile services.

3 Mandatory requirements for malicious communications

The following section gives an overview of malicious communications and outlines some mandatory requirements and best practice guidelines to limit their extent. It is intended that the mandatory requirements will be included as part of subsequent Content Standards control review to ensure compliance.

3.1 About malicious communications

Malicious personal phone calls have a long history. They are not restricted to the mobile environment and may affect customers of any age. However, the growth of mobile use among younger customers means that they are exposed to malicious personal communications more directly through their mobile than in previous decades when consumers could only be contacted through household fixed lines.

As the range of services offered by mobile network operators increases, the variety of potential malicious communications will also increase. We have already seen this with SMS. MMS and video services open the door to new visual forms of malicious communication. While not changing the basic phenomenon, these services may well be perceived by Vodafone customers as more intrusive or threatening than voice calls.

Examples of malicious personal communications include:

- Combining an offensive/threatening message with an image e.g. an image of an individual entering their home and the text message, "I know where you live"
- Violent images combined with a message e.g. an image of someone who has been beaten up with the text message "You're next"

Vodafone acknowledges that, despite best efforts, malicious communications will not be eradicated. However, effective and workable solutions can assist in resolving many of the problems associated with malicious communications.

3.2 Customer Support

It is a mandatory requirement that all Vodafone Operating Companies should update their existing malicious calls policies to cover all forms of malicious personal communications.

Customers should be left in no doubt that Vodafone is concerned about malicious personal communications and will assist them if they are subject to these. See Appendix I

Best practice processes include ensuring that details of Vodafone's Operating Companies' malicious communications policies and associated practical advice are clearly available on Vodafone's national website and through other customer collateral (leaflets etc) as appropriate. One potential route complementing the use of a web site would be to provide a recorded summary of advice via Vodafone's IVR systems or on a dedicated Vodafone free-phone number.

3.3 Police and law enforcement involvement

It is a mandatory requirement that all Vodafone Operating Companies should review their interaction with law enforcement agencies to make sure they have a clear escalation process that includes defined Vodafone responses in given circumstances and identifies reporting procedures. In particular: -

1. Once a customer's complaint has been processed by the police, Vodafone's Risk Management/Fraud and Security Department, or appropriate OpCo department, should assist in taking appropriate action against the person responsible.
2. If malicious communications are coming from Vodafone users we will take action under our contract to cease providing the relevant services to that user. If the malicious communications emanate from users on another network, Vodafone should identify the other network so that the police or other authorities can follow it up with them.

Following any subsequent investigation, criminal proceedings may take place. The customer may be required at some later stage to give evidence of the calls or messages in court. This should be made clear to the customer in advance.

3.4 Contractual measures

It is a mandatory requirement that all Vodafone Operating Companies shall ensure that their standard customer contracts prohibit the use of Vodafone's services for malicious communications. The terms should make clear that:

1. Malicious communications are prohibited.
2. Any complaints may be investigated and may involve Vodafone cooperating with the police or other authorities, including providing the police or other authorities, with evidence and information about the alleged offender.
3. Vodafone may terminate a customer's contract, or any particular service, if it is reasonably satisfied, having conducted investigations, that the customer has breached this prohibition, and that this right is not dependant upon the outcome of any formal proceedings by the police or other authorities.
4. Define what is meant by a malicious communication.

As many existing customers hold annual contracts, any revised amendments should be added when the contract is renewed.

Please refer to Appendix III, for text offered as a template to be used in standard customer contracts.

3.5 Malicious voice calls

Operating Countries should consider the following guidelines when reviewing malicious voice calls.

1. Vodafone should advise customers not to engage in conversation with an unknown caller as this may encourage further malicious calls. They should especially not reply when angry or upset, as this will often encourage the caller.
2. Customers who receive malicious calls should be advised to screen future incoming calls either by using Calling Line Identity (not answering calls with no CLI, or from numbers which they do not recognise) or by diverting all, or unrecognised, calls to voicemail. If voicemail is used, the customer should not record their own personal message but rather use the default "network-provided" message. They should ensure that they have enabled the security options on their voicemail and put in place a personal PIN to secure the voicemail. Alternatively, Operating Companies may offer a commercial personal message taking service - customers may be referred to this service for a period.
3. If a customer does receive a malicious call they should make a note of the call date and time, the caller's gender (if possible) and any other information about their voice or what they said. If the customer receives further malicious calls they should again record the same information. The customer should retain this information in case it is needed for any investigation or court proceedings.
4. If a customer calls Vodafone Customer Service, they should be advised that Vodafone can only record the details (not content) of the last incoming call made to a handset and therefore they should call Customer Services as soon as they have received a malicious call in order for it to be logged by the network. Customers should be advised not to delete any malicious messages, whether voice, SMS or MMS as they will prove helpful to the police in an investigation into a serious case. Customers should be able to authorise Vodafone, via Customer Services, to preserve and date relevant voicemail messages so that they can be made available to the police or relevant authorities should they wish to take matters further.
5. If Vodafone offers national phone book entries to mobile customers it is probably better that these do not include information on gender or whether customers are single or married. Female customers should be advised that it is better to use initials and last name rather than provide additional information. Note that in many countries the entries made into public directories are subject to legal requirements (such as providing the customer with the ability to determine what data about them is included) in order to protect the privacy of customers. Vodafone should ensure that, at the least, these requirements have been fulfilled.

3.6 Other types of malicious communications

Operating Countries should consider the following guidelines when reviewing other types of malicious communications.

1. As with voice calls, customers should not reply to malicious SMS, MMS, or video communications. They should especially not reply when angry or upset, as this will often encourage the sender.
2. Customers who receive malicious SMS, MMS or video should be advised to screen incoming messages¹ by examining the message Calling Line Identity (CLI) before opening the message. In particular, all SMS sent directly from another mobile handset will contain the originating handset CLI. If the customer has received malicious calls and receives a call from an unknown caller, then they can delete the message without reading it. SMS sent from Internet gateways may show no CLI – again, in this case, the customer can delete the incoming message without reading it.
3. If the customer has chosen to open SMS or MMS² communications from an unknown sender and these are malicious, then any decision by the customer to involve the police will require the customer to save the message, the number it is sent from, etc., in case they are needed as evidence.
4. Unless the process has been agreed by the legal department, if necessary in consultation with law enforcement bodies, customers should not be encouraged to save potentially illegal material (for example, a child abuse image), or to forward this to a third party as this may be illegal. This is an area where the best route to protect customers is not clear. Vodafone Operating Companies should be aware that the police or other authorities might wish to retain the handset as evidence. If this is the case, then advising the customer to retain the image may have the unintended consequence for them of the phone being retained if they contact the police. Where customers are subject to malicious MMS, a policy of deleting before opening MMS from unknown sources **may**, in reality, be the most effective way of suppressing this potential problem.
5. If a customer's mobile phone is held by the police as part of an ongoing investigation Vodafone Operating Companies could consider providing a replacement phone.

1 While phone design varies, customers subject to malicious non-voice communications will benefit from a modern phone which - typically - should offer screen-based CLI on incoming messages. The ideal option is a phone which shows message CLI without showing the message body. Some message text (such as subject) may be shown, but not the entire message text or enclosures. With MMS, a specific decision has to be made to download the message.

2 In principle, the same is true of network voicemail - which could be used subsequently to confirm a caller's identity. However, this then leads to a question of how easily the Vodafone Operating Company could identify and retain for a longer period, the specific customer's voicemails. An alternative approach would be for the customer to divert their mobile calls to a landline with an answer-phone on it. However, this would have additional call costs for the customer.

-
6. Where malicious communications are repeated, Vodafone should offer a change of number free of charge to reflect national expectations. For example, a number change could be offered
 - if the customer has reported malicious communication to the police
 - if a customer complains on more than one occasion about the same number
 7. Number change will be most effective in circumstances where the caller is not part of the complainant's social group. For example, it may address the situation of a malicious communications originator who has identified their victim at random. It is arguably much less likely to be effective in the area of *"text bullying"* between school children in the same class where a new number can be quickly communicated through the group.
 8. Customers who feel that their personal safety or the safety of another is in danger should be strongly advised to inform the police.

4 Mandatory requirements for bulk unsolicited communications (spam)

The following section gives an overview of bulk unsolicited communications and outlines some mandatory requirements and best practice guidelines to limit their extent. It is intended that the mandatory requirements will be included as part of subsequent Content Standards control review to ensure compliance.

4.1 About spam

Bulk unsolicited communications or spam, is now becoming a significant problem for mobile users. While spam has been traditionally confined to e-mail on the Internet, the development of new network services and the convergence of Internet and mobile services offered a simple transition to the mobile space that, if left, will have a significant impact on the business. For example, SMS spam in Europe is growing, while in Japan, over half the calls to Vodafone KK customer care are related to email spam.

For MNOs, the most pernicious form of current spam is unsolicited SMS soliciting a premium rate response, although voice examples also exist³. In both cases, the intent is to encourage customers to respond to a premium rate voice, or SMS service.

Vodafone passes on part of the premium to the end “service provider” company usually linked to the sender of the original unsolicited message. This payment is often via a number of intervening communication providers the last of which will have the contract with the operator of the premium rate service/number. For premium rate SMS, payment may be made via an SMS aggregator that has a contract with Vodafone. For premium voice, payment is often made via another telco (normally the fixed ex monopolist), which has a contact with Vodafone.

Examples of mobile spam include:

- An SMS, or email, designed to advertise a service delivered to a mobile handset;
- An SMS, or other mobile communication to solicit a premium rate response; and
- A “one ring” voice call designed to solicit a premium rate response:

Spam is not typically directed at younger customers and does not require specific measures for this group. However, younger customers are likely to be a flashpoint for customer, media, pressure group and regulatory concerns. This is already the case with pornographic spam on email. To avoid compromising new mobile services it is important that Vodafone acts to suppress the transition of this problem to mobile.

³ Examples of voice spam are “missed calls” or “one-ring calls” which leave premium rate CLI on a customer’s phone.

4.2 National regulatory support

Vodafone believes that the mobile industry has an important role in developing effective and workable solutions to address the problem of mobile spam. In developing these solutions, Vodafone will seek to work alongside other interested parties including government bodies, the marketing industry and consumer groups.

Any effective solution needs to combine regulatory, self-regulatory, technical and consumer approaches. Experience has shown that any attempted solution that fails to combine these considerations, such as a simple legal ban on "unsolicited marketing" will not work⁴.

The reason that a legal approach is ineffective on its own is that spam is not typically sent by responsible people. It is sent, often internationally, by people who are generally breaking the law in a range of other ways and are indifferent to national legal prohibitions on unsolicited messages.

However, a common enabler of action against malicious and unsolicited bulk communications is the creation of a national policy consensus that these activities are illegitimate.

In light of this, it is a mandatory requirement for Operating Companies to:

- Support the outlawing of malicious personal communications. Vodafone should lobby for legislation which is consistent and technologically neutral to capture new forms of mobile services and which includes effective sanctions, both civil and criminal for companies and individuals that break the law.
- Support permission based marketing regimes covering all electronic services. Legislation should include effective sanctions for companies and individuals who breach these.
- Support specific legal or regulatory prohibitions on using premium rate numbers in Caller Line Identity or in the body of the message for voice, SMS or other forms of communication where these messages are unsolicited.
- Obtain regulators' support for robust commercial and regulatory action against national and international senders of bulk unsolicited communications who ignore a permission based marketing regime – particularly where they are soliciting a premium rate response and/or are using premium rate numbers in CLI.
- Where permission based framework is in force, Vodafone should comply with it in all relevant written and electronic communications with customers.

4.3 Unsolicited SMS soliciting a premium rate response

Experience in the UK has shown that a reporting procedure has had a significant effect on reducing spam. It is therefore a mandatory requirement that all Operating Countries provide customers with a procedure to allow them to report spam that they receive on their mobiles.

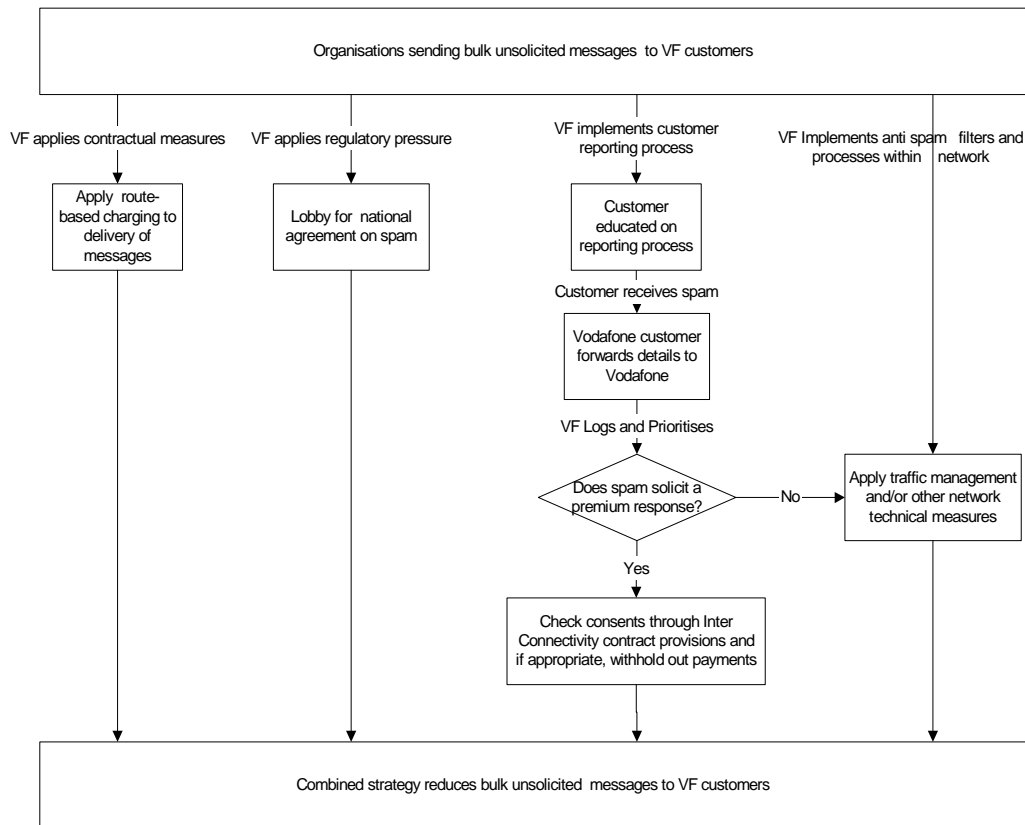
⁴ Many countries have adopted legislation that outlaws spam which is technologically neutral and therefore relates to SMS, MMS and other forms of mobile messaging.

One way for Operating Companies to do this is to provide customers with an automated reporting facility. This would:

- Operate as a single, dedicated short code to which spam can be forwarded free of charge e.g. Vodafone UK offers VSPAM (87726) but SPAM (7726) might be a better choice for a cross industry short code.
- Support the reporting of spam on new mobile messaging such as MMS and video messaging on the same short code.
- Be extendable to other messaging services by using relevant addressing e.g. vspam@vodafone.co.country or spam@vodafone.co.country for Vodafone brand email.

It is a mandatory requirement that all Operating Companies make SMS, or other messages soliciting a premium rate response, economically unviable. The approach Vodafone advocates is essentially to undermine the economic viability of SMS spam soliciting a premium rate response.

4.4 Stamp out SMS spam by making it uneconomic



A recent development in relation to SMS spam is "spoofing" where internationally originated SMS fraudulently include message header information from third party operators. This is now the subject of a GSMA technical working group.

Vodafone Group supports this measure and is involved with this working group.

It is sometimes possible to identify countries that are originating spam by comparing the outbound and inbound traffic, i.e. spammers tend to be located in situations where the outbound traffic greatly exceeds the inbound.

While, in principle Vodafone Operating Companies should be free to compete with other operators (and potentially with each other) for internationally originated bulk SMS, there are good reasons why it is in Vodafone's (and the mobile industry's) overall interests, that bulk SMS containing premium rate numbers is only originated nationally.

In particular, a reasonable suspicion must be that the reasons for sending such bulk SMS internationally are either:

- to take advantage of price variations between national bulk SMS rates and the international interworking rate;
- that the sending company is seeking to originate SMS from outside the legal/regulatory environment of the destination territory in order to avoid national regulatory controls on the sending of unsolicited messages which operators in the destination countries would apply; or
- that the sending company is seeking to originate SMS from outside the legal/regulatory environment of the destination territory, soliciting a premium rate response, in order to avoid national regulatory controls on premium rate services which operators in the destination countries would apply.

Vodafone should compete for this kind of SMS traffic on a national basis - so that we are able to apply effective controls on SMS abuse. Hence, we should not carry this traffic internationally.

4.5 Adoption of calling party pays

It is a mandatory requirement that Operating Companies should adopt the "calling party pays" principle, when the customer is charged for sending a message (i.e. the Vodafone Internet Protocol Commercial Model) for new mobile services. This will have a positive effect in limiting bulk unsolicited communications.

A meaningful termination charge will create a cost barrier to the sending of spam and enable us to avoid the fixed email experience where spam is now dominating message volumes. Vodafone Group should therefore apply calling party pays commercial approaches to termination of all new forms of mobile calling and message services.

Where, for tactical reasons, a Vodafone Operating Company launches a new mobile service without an appropriate termination billing capability, the contractual framework should, nevertheless, include provision for payment using the IPCM.

4.6 Customer contracts

It is a mandatory requirement that Vodafone Operating Companies should ensure that their standard customer contracts prohibit the use of Vodafone's services for initiating or sending spam. The terms should make clear that:

1. Unlawful activity, including the sending of unsolicited communications for fraudulent purposes, or for marketing, or advertising purposes, without lawful grounds, is prohibited.

2. Any complaints may be investigated and may involve Vodafone cooperating with the police or other authorities, including providing the police or other authorities, with evidence and information about the alleged sender.

Vodafone may terminate a customer's contract, or any particular service, if it is reasonably satisfied, having conducted investigations, that the customer has breached this prohibition, and that this right is not dependant upon the outcome of any formal proceedings by the police or other authorities.

Please refer to Appendix III for text offered as a template to be used in standard customer contracts.

4.7 Interconnection / Interworking

It is a mandatory requirement that all terms of interconnection and interworking agreements need to be reviewed to ensure that they provide Vodafone with the contractual right to withhold out-payments to intervening communications providers in respect of premium rate services where a customer has complained that they have received unsolicited SMS soliciting a premium rate response. Where contracts do not provide sufficient rights to do so, they should be amended. To the extent that intervening communications providers are unwilling to agree such amendments, Operating Companies should seek support from national regulatory authorities for such changes.

In this respect, the GSMA has prepared an Addendum to the International GSM Roaming Agreement (SMS Interworking Agreement: Official Document AA.19) to counter the effects of SMS spam. In particular, this operates by discouraging the international transmission of SMS which are either unsolicited or which encourage responses to premium rate services. It allows a GSM operator to terminate its international links with another GSM operator that is originating SMS messages that fall into these categories, or are otherwise unlawful or fraudulent. Operating Companies should consider incorporating this Addendum in their roaming agreements.

4.8 SMS content and PRS provider agreements

It is a mandatory requirement that the terms of existing bulk SMS content and PRS provider agreements should also be reviewed to ensure that they provide Vodafone with the contractual right to take action against the sending of spam. Please refer to Appendix III for text offered as a template to be used in standard bulk SMS content provider/PRS provider contracts. In addition, for contracts with PRS providers, Operating Companies should ensure they have the contractual right to withhold outpayments where a customer has complained that they have received unsolicited SMS soliciting a premium rate response.

4.9 Technical solutions

Where it is not possible or sufficient to use a calling party pays charging regime, Vodafone should consider the adoption of message filtering. There are legal restrictions concerning the operation of message filtering, which need to be discussed with Operating Companies' legal departments or Group Legal. However, Vodafone should take note of industry practice, particularly the practices of the fixed ISPs in any particular market, and the views and opinions of Government and regulators. As there may be a mismatch between the strict legal regime and the expectation of Government and other stakeholders regarding Vodafone's responsibilities to tackle spam.

Any national Vodafone brand email service must offer the type of anti spam protection that is already established good practice for the fixed internet.

SHARK, (see Appendix II) is a network based anti spam tool developed by Vodafone Spain. It has been offered to a number of other Operating Companies in as a further measure in the fight against spam where it is not being controlled by regulatory or commercial means.

4.10 Group Marketing support

Group Marketing will provide product management support for spam protection on its MMS service and will take an active role in liaising with technical forums such as Global Group Security and Fraud Forum and Global Fraud Risk & Security Council. This includes the presentation of OpCo's comments and needs and sharing outcomes across the business.

If local circumstances dictate, Operating Companies are asked to develop and implement their own technical solutions for Mobile Party Pays services (e.g. Pull/Push email) and SMS.

5 In summary

The following table summarises the key mandatory requirements and best practice guidelines for compliance with the malicious and unsolicited calls policy and identifies contacts within Vodafone Group who can offer advice concerning implementation.

Action	Process	Group Contact
<p>Review existing malicious communications procedures and update documentation to take into account new types of communications including, but not restricted to, MMS, SMS, video messages and video calling</p>	Mandatory	<p>Antonio Morawetz</p> <p>Customer Operations Director</p>
<p>Review and if necessary amend standard contracts to ensure that standard contracts prohibit the use of Vodafone services for initiating or sending spam.</p> <p>Opcos should review all terms of interconnection and interworking agreements to ensure Vodafone has the right to withhold outpayments.</p> <p>OpCos should review terms of existing bulk sms and PRS provider agreements to ensure they provide contractual right to take action against the sending of spam</p>	Mandatory	<p>Stephen Deadman</p> <p>Senior Solicitor, Group Legal</p>
<p>Establish unsolicited communications procedures. Vodafone Operating Companies should make bulk unsolicited SMS soliciting a premium rate response economically unviable as a matter of priority</p>	Mandatory	<p>Nick Mann,</p> <p>Head of Fraud, Risk and Security</p>
<p>Customer education. Provide a facility so that customers can easily report Spam to Vodafone</p> <p>Ensure customers are aware of how to respond to personal malicious communication and to report spam and malicious communication</p>	<p>Mandatory</p> <p>Best Practice</p>	<p>Antonio Morawetz</p> <p>Customer Operations Director</p>
<p>Obtain regulators' support for robust commercial and regulatory action against national and international senders of bulk unsolicited communications soliciting a premium rate response</p>	Best Practice	<p>Rob Borthwick</p> <p>Public Policy Executive</p>
<p>Implement Calling Party Pays (Internet Protocol Commercial Model) for new mobile services to launch with a specific termination regime in place. Tactical launch considerations may delay actual billing, but not contractual framework</p>	Best Practice	<p>Ralf Mackes</p> <p>Commercial Model Competence Centre</p>
<p>Review key technical measures for products at network level. Message filtering should be deployed where commercial or regulatory solutions are not available or effective. There are legal issues with the implementation of message filtering, however, Vodafone should consider the legal precedents set by national fixed ISPs and the views of the course, regulators and Government</p>	<p>Pending publication of Messaging End Game Policy</p>	<p>George Power</p> <p>Head of Messaging</p>

APPENDIX I - Vodafone Ireland case study

Vodafone Ireland co-operates with the Irish law enforcement authorities directly or indirectly on approximately 100 cases of malicious communications each month.

As the technology usage by Vodafone customers grows, the increase in malicious communications will increase. In acknowledgement of this, Vodafone Ireland has reviewed its policies in order to keep up with the technological innovation and expected concerns.

At present VF Ireland has:

- A specific route for customers to report malicious communications – through all customer care desks with possible escalation to VF Ireland's Risk Management area
- A documented internal policy for handling malicious communications that is communicated to customers and staff through VF Ireland's web-site.
See : <http://www.vodafone.ie/aboutus/practice/policies/>
- Put in place contractual measures. Customer terms and conditions refer to proven incidences of malicious communications by a customer as a reason to terminate their service on the Vodafone network

Procedures for dealing with nuisance calls/messages

Vodafone Ireland has always assisted the Garda Siochana (the Irish police services) whenever a prosecution is being contemplated regarding the transmission of nuisance, threatening or offensive text messages via mobile phones.

- Vodafone Ireland has an agreed customer care agent script for dealing with a customer who is calling to report malicious communications
- A customer feeling aggrieved as a result of receiving a nuisance, threatening or obscene call or message should be advised to report the matter to the police authorities in the first instance
- A customer complaining of offensive SMS or other messages should be advised to retain the message (by storing it within the archive memory in the phone) for use as evidence.

Once they have been contacted, the police authorities will conduct an investigation and, when satisfied that a breach of the relevant section has taken place, they will send a file on the matter to Vodafone.

Public position

Vodafone Ireland has a clear public position statement with respect to malicious communications. This is used for dealing with press enquiries. It states:

“It is Vodafone's policy to assist the Garda Siochana on their request whenever a customer has reported an incident of nuisance or threatening text messages.

It is a criminal offence:

‘The transmission of nuisance, threatening or offensive text messages on mobile phones is covered by existing legislation - Post Office (amendment) Act, 1951/ as amended by Postal 7 telecommunications services Act 1983/1999.’

If a person, (a) sends any message by telephone which is grossly offensive or of an indecent, obscene, or menacing character; (b) sends any message by telephone which he knows to be false, for the purpose of causing annoyance, inconvenience, or needless anxiety to any other person or (c) persistently makes telephone calls without reasonable cause, for any purpose as aforesaid, he shall be guilty of an offence.

We would advise anyone receiving offensive text messages to:

- Store the message on the phone's memory, for evidential purposes
- Contact the police services who will take details such as text messages and sender's number
- The police will conduct an investigation and if satisfied that a breach of the relevant Acts has taken place then they will decide whether to prosecute or not

“Where an offensive SMS message originates from a Vodafone number the company may, following adequate investigation, restrict or remove SMS service according to our Terms & Conditions of service”

Customer education

VF Ireland has produced specific advice on bullying and malicious communications for customers. This can be found on VF Ireland's web-site at:

<http://www.vodafone.ie/aboutus/practice/policies/bully/>

It has also cooperated with other Irish MNOs to produce a Code of Practice on content including a parents' guide. See the guide at:

<http://www.vodafone.ie/aboutus/practice/iciaguide/>

Customer terms and conditions

Where offensive SMS messages originate from a Vodafone mobile phone, the company may, following adequate investigation, restrict or remove SMS service according to Terms & Conditions of service.

*“The services are made available to you on the basis that you or any other party using the service with your express or implied consent or for whose use of the services you are responsible
(a) Will not use the services for any improper or unlawful purpose or allow others to do so;
(b) Will comply with all relevant legislation or regulations relating to the use of such equipment and the use of the services”*

Customer care script

I'm sorry to hear that you are receiving these unwanted communications. There are a few steps that I can advise you to take:

If you receive any more calls, log the call time, the date and any other information about the call. It is important not to engage in conversation or reply to the caller, as this will only encourage more nuisance communications.

If you receive any more text messages, save the messages or archive them on your phone. You may need this information if you decide to take it further at a later stage.

If the calls are persistent and are causing needless anxiety, we can offer you a change of number free of charge on receipt of a complaint from yourself that is stamped by the Police.

If the customer is not happy with this and wants to take it further:

If the problem calls continue it may be necessary to have the matter investigated by the police.

If you decide to report it to the police, you will be required to make a written statement of the complaint and give permission to have your phone records checked. If you are not the account holder of the phone, the police will need the written consent of that person. The police, through their channels, will process your complaint and our Risk Management Department will assist them in trying to identify the person responsible.

If the calls are emanating from another telecom network the police will follow it up with them. In the case of text messages, the police will need to record the message, the number it is sent from etc. - this is the reason why it is so important that you save these details.

If in the event that the Police trace the identity of the caller/sender and after an investigation it may be decided to take criminal proceedings - you may be required at some later stage to give evidence of the calls or text messages in court.

APPENDIX II - SHARK initiative

SHARK is a network based anti spam tool developed by Vodafone Group in 2001. It is capable of real-time content filtering based on customer specific profiles – a key tool in suppressing spam.

The SHARK initiative was originally a concept project to limit the amount of spam our wireless subscribers receive. The project was moved to Vodafone Spain for final testing and initial European deployment.

SHARK has been in full production trial since October 2003 with more than 100 million messages filtered and a 60% average daily rejection rate.

SHARK has real time statistical monitoring to allow quick interaction to spam attacks as well as extensive management reporting.

It is specially designed for the needs of the wireless subscriber using “state of the art” technology. It has a very low cost of ownership with no annual software fees.

The installed system is capable of supporting a very large number of Vodafone Operating Companies at very low additional cost. VF-ES will provide this service to any operator on request.

Customers have been very receptive to the SHARK system, as the volume of spam has been reduced with no reported problems.

APPENDIX III – Contract clause template

The following text is offered as a template (with any appropriate modifications as deemed appropriate by the operating companies' legal departments) to be used in standard customer and content / PRS provider contracts:

1. The use of Vodafone's services, including voice, SMS, MMS, video, or other messaging or communication services, offered now, or at any time in the future, for the purpose of creating, initiating or sending:
 - a. malicious communications; or,
 - b. unsolicited communications for fraudulent, deceptive or misleading purposes;
 - c. unsolicited communications for marketing or advertising purposes without lawful grounds,

is prohibited.

2. Any complaints made against [the customer] in respect of the above may be investigated and may involve Vodafone cooperating with the police or other authorities, including providing the police or other authorities with evidence and information about [the customer] and the complaint.
3. Vodafone may terminate [the customer's] contract, or any particular service, if Vodafone is reasonably satisfied, having investigated the complaint, that [the customer] has breached the prohibitions in Clause [1] above. This right of termination is not dependant upon the outcome of any proceedings by the police or other authorities.
4. "Malicious communication" means any call or message that is intended to cause, or has the effect (as such may be contemplated by a reasonable person) of causing, the recipient to feel harassed, abused or offended.