smartCommunicator® Acceptable Use Policy

The smartCommunicator® Acceptable Use and Security Policy (this "***Policy***") applies to smartCommunicator clients ("***Clients***") and operators of smartCommunicator ("***Operators***").

1. Consent. A Client may only send email messages to an individual who (i) has provided Authorized to receive email from the Client or (ii) has an existing business relationship with the Client.

(a) Authorized is defined as the Recipient expressly consenting to receive the message, either in response to a clear and conspicuous request for such authorized or at the Recipient's own initiative. Clients may obtain Authorized as follows:

Confirmed Opt-in

Following an opt-in request, a confirmation email is subsequently sent to the person notifying him that some action is necessary before his email address will be added to the list. The person must respond or take other equivalent action to be considered "confirmed."

Notified Opt-in

At the point of email address collection, a person has requested to be included on an email list to receive email. An email is subsequently sent to the person, notifying the person that his or her email address has been added to the email list. The person is not required to take further action to be included on the email list.

Opt-in

At the point of email address collection, a person has requested to be included on an email list to receive email. No confirmation email is sent and the person is not required to take further action to be included on the email list. Obtaining Authorized through the means described in this clause (iii) is discouraged by smartCommunicator and Clients are encouraged to discontinue obtaining Authorized in this manner as it may be prohibited by smartCommunicator in a future revision to this Policy.

A "clear and conspicuous" request for authorized to receive email means that the person from whom authorized is being requested must be required to take an action (such as checking a box or radio button) that is specifically associated such consent. Pre-selection of a box or radio button requesting consent, or authorized that is included within terms of service or use that are consented to by an action, but where the action is not specifically linked to the authorized to receive email, does not constitute a clear and conspicuous request for consent.

In jurisdictions where email communications are subject to a more restrictive definition of authorized (e.g., the European Commission Privacy and Electronic Communications Directive), Clients shall adhere to the applicable local standards.

(b) Existing Business Relationship. A business relationship between a Client and a Recipient may be created through the facilitation or completion of a transaction.

(c) Affiliate Marketing. The smartCommunicator service may not be used for affiliated marketing campaigns unless smartCommunicator has expressly approved any such use of affiliate marketing by Client in writing, which approval may be withheld or subjected to conditions established by smartCommunicator in its sole discretion.

Prohibited Practices

(i) List Sharing; Co-Registration. The smartCommunicator service may not be used for co-registration, list rental, list exchange, partner mailings or similar types of email campaigns and emails addresses collected through such practices may not be used with the smartCommunicator service.

(ii) Lack of Control over Recipient or Content. The smartCommunicator service may not be used for email over which the Client does not possess control over content and choice of recipient. For example, a "forward-to-a-friend" email (where an email recipient or web site user chooses the recipient) would not be available for use with the smartCommunicator service.

(iii) Email Prospecting. Any form of email prospecting (i.e., where there is no authorized or existing business relationship between the Client and the Recipient) using the smartCommunicator service is prohibited.

(iv) Other Prohibited Practices. Email addresses to be used for the smartCommunicator service must not be gathered through surreptitious methods (e.g., scraping, harvesting, or dictionary-style attacks).

Content

Clients shall ensure that all smartCommunicator service conform to all applicable laws including, but not limited to, the CAN-SPAM Act of 2003. In addition, smartCommunicator service shall comply with the following:

(a) Message headers, subject lines and content shall not be misleading, misrepresentative or falsified in any way.

(b) Messages shall not transmit viruses or other programs which may destroy or limit the functionality of a computer.

(c) Messages shall not contain content which is unlawful or harassing.

3. Unsubscribe.

(a) Inclusion in Email. Clients shall include an unsubscribe function within each smartCommunicator service that does not fall within the definition of "Transactional" (see Section 5 – smartCommunicator service Token Classifications). All smartCommunicator service that fall within the definition of "Transactional" must contain an unsubscribe function if required by applicable law. The unsubscribe function must be easy to use and must be clearly and conspicuously located in the email. In addition, the unsubscribe function:

(i) must remain active and functional for at least 30 days after the message is sent,

(ii) must be processed within 10 business days of receipt (or such shorter period of time if required by applicable law), and

(iii) must not require a Recipient to provide any information other than the Recipient's email address (unless the Recipient has been clearly and conspicuously notified at the point of collection that receiving such Email Messages is a requirement to receive a service).

The requirements of this Section 3 apply to all smartCommunicator service regardless of the Token class used for the smartCommunicator service.

(b) Permanence of Unsubscribe. Once an unsubscribe request is received, it shall be considered permanent and no smartCommunicator service may be sent to that Recipient unless Authorized is obtained again; provided that Recipient may send smartCommunicator service falling within the definition of "Transactional" (see Section 5 – smartCommunicator service Token Classifications) to such Recipient if the smartCommunicator service for which the unsubscribe request was received did not fall within the definition of "Transactional" (or vice versa) and it is otherwise permitted under applicable law. Re-establishment of a business relationship is not sufficient to override a prior unsubscribe request.

(c) Complaint as Unsubscribe. Unless otherwise indicated, smartCommunicator will interpret a complaint (e.g. a Recipient clicking "This is Spam") as a request to unsubscribe and expects Clients to unsubscribe a complaining Recipient. smartCommunicator will identify complaining Recipients to Client for this purpose.

(d) Acknowledgment. Client acknowledges that in order to process unsubscribe requests and complaints received through the smartCommunicator service, mailbox providers will provide complaint data and email addresses of complaining Recipients to smartCommunicator in order for smartCommunicator to provide this information to Client.

4. Accreditation.

(a) Application. Prospective Clients must successfully complete accreditation process before sending smartCommunicator services. Prospective Clients must complete an accreditation application, which will be reviewed by a representative of smartCommunicator or one of its accreditation partners, after which an accreditation decision will be rendered.

(b) Limited Accreditation. Clients may be accredited with use limitations until such time, as determined by smartCommunicator, that such use limitations are no longer necessary. By example, and not by way of limitation, use limitations may include (i) smartCommunicator service sending limits (quotas), (ii) limited/no use of the smartCommunicator service icon and marks and (iii) registration of "from" lines with smartCommunicator for monitoring.

5. smartCommunicator service Token Classifications.

(a) Classifications. smartCommunicator will provide a mechanism to designate smartCommunicator service as being within a particular Token class. The Token class of a smartCommunicator service designates the purpose of the email and determines the unique set of features and functions that will be available to Clients, Operators and Recipients with respect to that email. Clients and Operators shall ensure that all Messages meet all requirements of the Token class used and are marked as the appropriate Token class." smartCommunicator may add additional Token classes in the future.

(i) Standard: This default category is intended to be used for most email, including commercial email. The Standard Token class may be used with any email message that does not violate this Policy. The Standard Token class will enable only base smartCommunicator service features and functionality. Enhanced features and functionality available with other Token classes requires the use of that Token class.

(ii) Transactional: This Token class may only be used for email messages where the primary purpose of the email message is:

(1) to facilitate, complete or confirm a commercial transaction that the Recipient has previously agreed to enter into with Client;

(2) to provide warranty information, product recall information or safety or security information with respect to a commercial product or service used or purchased by the Recipient;

(3) to provide:
(a) notification concerning a change in the terms or features of,
(b) notification of a change in the Recipient's standing or status with respect to, or
(c) at regular periodic intervals, account balance information or other type of account statements with respect to a subscription, membership, account, loan, or comparable commercial relationship involving the ongoing purchase or use by the Recipient of products or services offered by the Client;

(4) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or

(5) to deliver goods or services, including product updates or upgrades, which the Recipient is entitled to receive under the terms of a transaction that the Recipient has previously agreed to enter into with the Client.

The definition of "Transactional Email" is intended to mirror the definition of "Transactional or Relationship Message" in the CAN-SPAM Act of 2003 and the regulations promulgated there under. The Transactional Token class will enable only base smartCommunicator service features and functionality. Enhanced features and functionality available with other Token classes will require the use of that Token class
(iii) CE Paper Suppression: In addition to the base smartCommunicator service features and functionality, this Token Class includes the storage of hash of email messages for no repudiation purposes. The CE Paper Suppression Token class may be used with any email message that does not violate this Policy.

(iv) Certified Video. In addition to the base smartCommunicator service features and functionality, this Token Class provides sender with the ability to include playable streaming video content inside email messages. This Token Class may be used for an email message only if the video content either (A) is received by the email recipient as a still image that must be clicked by the recipient to run or (B) is received by the email recipient running on mute and must be clicked by the recipient to add sound and the email message does not otherwise violate this Policy. For purposes of clarification, video content included in an email message is considered content of that email message and subject to the requirements of this Policy with respect to email message content.

(v) Certified Video Editorial: In addition to the base smartCommunicator service features and functionality, this Token Class provides the sender with the ability to include playable streaming video content inside email messages. Email messages using this Token Class must meet the requirements for the Certified Video Token class. In addition, the video content must not include third party advertising, whether pre-roll, post-roll or embedded in the content. Third party image and text advertisements in the email message itself are permitted. For purposes of clarification, video content included in an email message is considered content of that email message and subject to the requirements of this Policy with respect to email message content.

(vi) CE Timed Delivery: In addition to the base smartCommunicator service features and functionality, this Token Class provides sender with the ability to specify a desired time of delivery for the email message. The CE Timed Delivery Token class may be used with any email message that does not violate this Policy.

(b) Class Selection. Clients and Operators may use any Token class with an email message, so long as the email message meets the criteria for use of that Token class set forth above, provided that features and functionality that are enabled by a particular Token class will not be available if another Token class is used. For example, the "Standard" Token class could be used for email messages that would qualify for "Transactional" classification if so desired, but the "Transactional Email" Token Class could not be used for email messages that do not meet the requirements for use of the "Transactional" Token class.

(c) Additional Restrictions. Additional limitations on the availability of Token classes, including without limitation for use with particular smartCommunicator mailbox provider partners, may apply. In addition to obtain the benefit of enhanced features and functionality provided with certain Token classes sender may be required to take additional actions or comply with additional usage guidelines. For further information with respect to a Token class, see current published documentation for the Token class.

6. Account Identification Codes. Each Client and Operator will be assigned one or more account identification codes. Account identification codes are used to identify (i) the sender of a Message, (ii) the party responsible for payment for a Message and (iii) in the case of an ESP, on whose behalf a Message was sent. Failure to properly use identification codes inhibits Good mail's ability to measure Client accountability and is considered a material violation of this Policy. Account identification codes may only be used by and on behalf of the entities to whom they are assigned. Use of any account identification code on behalf of a party to whom it was not assigned will be a material violation of this Policy. An Operator shall not send smartCommunicator service on behalf of any Client unless (A) the Client has agreed to comply with Good mail's Terms of Use and this AUP in connection with establishing an account with, (B) the Client has entered into a separate agreement with smartCommunicator for the purchase of Tokens that requires use of such Tokens to comply with this AUP or (C) Operator is a reseller to Client of the Tokens used in such smartCommunicator services, and has entered into a reseller agreement with smartCommunicator that requires use of such Tokens to comply with this AUP . Clients and Operators shall not provide their account identification codes to any other party (except Client may provide its account identification codes to an Operator who is authorized to send smartCommunicator service on Client's behalf). Use of incorrect account identification codes or misuse of account identification codes shall be considered a material violation of this Policy and may be cause for suspension of Client or Operator accounts or termination of a Client's or Operator's agreement.

7. Recipient Complaints and Reputation Score

(a) Complaints. A complaint occurs when smartCommunicator receives notice from a Recipient regarding an unwanted message. Unless the level of granularity of a complaint indicates otherwise, smartCommunicator will interpret a complaint as a request to unsubscribe and expects Clients to unsubscribe a complaining Recipient. smartCommunicator will identify complaining Recipients to Client for this purpose.

(b) Reputation Scores. Each Client will have Reputation Scores calculated by smartCommunicator. A Client's Reputation Scores are based on the Client's smartCommunicator service complaints normalized across participating mailbox providers over 12-week, 4-week and 1-week periods. Additionally smartCommunicator will track Client's unsubscribe practices through "repeat complaints" and "unsubscribe days". smartCommunicator reserves the right to change the method of calculation of the Reputation Scores at any time. Clients should strive to keep their Reputation Scores as low as possible at all times. Client acknowledges that (i) smartCommunicator owns Reputation Score data, (ii) smartCommunicator may share Reputation Score data with third parties as reasonably necessary for legitimate business purposes and (iii) smartCommunicator may publish Reputation Score data on an anonymous or aggregate basis.

(c) Maximum Scores. The Maximum Scores represents an upper limit for acceptable Reputation Scores. If a Client's Reputation Score for a 12-week period or a 4-week period exceeds the Maximum Score applicable to such period, smartCommunicator will place the Client's account (with respect to the applicable Token class) on probation and notify the Client. If a Client's Reputation Score for a 1-week period exceeds the 1-week Maximum Score, Client's account (with respect to the applicable Token class) will be terminated. The Maximum Scores will be posted and may be changed by smartCommunicator at any time.

(d) Calculation and Notification. Reputation Scores will be calculated on a weekly basis and posted in the Client's account. Client will receive a notification if any of its Reputation Scores exceeds 80% of the applicable Maximum Score.

8. Probation and Termination

(a) Commencing Probation. smartCommunicator shall place a Client's account (with respect to a particular Token class) on probation if either of Client's Reputation Scores at any time exceeds the applicable Maximum Score or for any other material violation of this Policy. The length of time during which a Client's account will be on probation (the "**Probation Period**") is four (4) weeks. During the Probation Period, Client's smartCommunicator Token prices will be increased by twenty-five percent (25%). Subject to Section 10, the Probation Period pricing penalty may be modified from time to time.

(b) Successfully Completing Probation. At the end of the Probation Period, Client's account will no longer be on probation:

(i) where the Probation Period was triggered by Client exceeding the 12-week Maximum Score, if Client's 4-week Reputation Score is less than Client's 12-week Reputation Score (indicating improvement); *provided, however*, that if Client's 12-week Reputation Score still exceeds the 12-week Maximum Score at the end of the Probation Period, Client shall begin another Probation Period (not to exceed three consecutive Probation Periods, including the first); or

(ii) where the Probation Period was triggered by Client exceeding the 4-week Maximum Score, if Client's 4-week Reputation Score is less than the 4-week Maximum Score; or

(iii) where the Probation Period was triggered by Client's violation of this Policy not described in Section 8(b)(i) or (ii), such violation is remedied to the reasonable satisfaction of smartCommunicator.

(c) Unsuccessfully Completing Probation; Termination. Except as described in Section 8(b)(i), at the end of the Probation Period, Client's account (with respect to a particular Token class) will be terminated if Client does not successfully complete Probation.

Mailbox Provider Notification

smartCommunicator will provide its mailbox provider partners with immediate notification of Clients who are placed on probation or whose use of the smartCommunicator service has been terminated.

Special Circumstances

If a Client (i) exceeds the 4-week Reputation Score more than once within a 12-month period, (ii) fails three consecutive Probations for violation of the 12-week Maximum Score or (iii) posts a 1-week Reputation Score in excess of the 1-week Maximum Score, Client's account (with respect to a particular Token class) will be terminated. In addition, in order to protect the smartCommunicator service, smartCommunicator mailbox provider partners and their members, smartCommunicator reserves the right to immediately and without notice terminate a Client's account with respect to any or all Token classes, suspend a Client's access to the smartCommunicator service or take such other action in its discretion in the event that (A) Client's behavior or complaint level (measured over any period) indicates that a material violation of this Policy is likely to have occurred or be in the process of occurring , (B) Client acts unlawfully in relationship to the smartCommunicator service, smartCommunicator mailbox provider partners and their members or (C) continued use of the smartCommunicator service by Client would damage the reputation or otherwise not be in the best interests of the smartCommunicator service, smartCommunicator or any of its mailbox provider partners or their members, in each case as determined by smartCommunicator in its sole discretion. Neither Client nor any Operator shall have any recourse against smartCommunicator or any of its mailbox provider partners or their members in the event such action is taken.

Reinstatement/Reaccreditation

If a Client whose use of the smartCommunicator service was previously terminated can demonstrate to smartCommunicator that it has taken appropriate corrective action, smartCommunicator may reinstate the Client with appropriate use limitations until the Client reasonably satisfies smartCommunicator that its email practices comply with this Policy and that its future Reputation Score is not reasonably likely to exceed the Maximum Score. Decisions on reaccreditation and applicable use limitations will be determined by smartCommunicator on a case-by-case basis together with Client, but will ultimately be determined in Good mail's sole discretion. By example, and not by way of limitation, use limitations may include:

(i) smartCommunicator service sending limits (quotas)

(ii) Limited/no use of the smartCommunicator service icon and marks

(iii) Pre-registration of "from" lines with smartCommunicator for monitoring

9. Security.

Account Security

Clients and Operators shall ensure that all user names and passwords used to access smartCommunicator shall be carefully safeguarded and not distributed or shared with any unauthorized individual. The account identifiers within the smartCommunicator should be treated as confidential information and should not be disclosed or provided to any third party outside of the Client's or Operator's security organization (with exception for contractors as noted below). Client shall immediately notify smartCommunicator if anyone obtains Client's account information or accesses Client's account without permission.

Integrity of Tokens

Clients and Operators shall not modify, translate, disassemble, decompile, reverse engineer, or otherwise attempt to discover the source code of smartCommunicator Tokens or other smartCommunicator proprietary technology.

Support

Operators shall provide and make available a dedicated security support contact or contacts who can be reached with security questions or concerns twenty-four (24) hours a day, seven (7) days a week. Operators may change the name or contact information for this dedicated security support contact by providing notice to smartCommunicator at the .

Virus Precaution

Operators shall ensure that all networks, databases, computers and software utilized to send smartCommunicator service (and the smartCommunicator service themselves) are checked with industry standard up-to-date antivirus software, and are determined to be virus-free prior to sending smartCommunicator services. Operators shall update virus definitions at a sufficient cadence to ensure that they use the most up-to-date definitions available, and will conduct virus sweeps, at an industry standard frequency, of all networks, databases, computers, and software (including archival copies of the foregoing) utilized to send smartCommunicator services. Operators shall promptly purge all viruses discovered during such sweeps. If an Operator discovers that a virus may have been transmitted via Email, Operator shall promptly notify smartCommunicator of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Operator has used to purge the virus.

Systems Security

System Adequacy

Operators shall have obtained and configured adequate hardware, software, power and human capital redundancies to send Email messages. The Operator's facility shall be properly configured to industry standards, including, but not limited to preventing open proxies, open relays and closing all known and published security deficiencies therein, and permitting access thereto only to authorized personnel, subject to password protection.

Firewall

Each Operator certifies that it has implemented and will maintain continuously industry standard firewall protection for all of its networks, databases, and computer systems. Operators shall update firewall software promptly when updates become available. In addition, Operators shall log attempted accesses to their networks, databases, and computer systems, and the result of such attempts, and will review and assess such firewall and web server access logs at an industry standard frequency. Operators shall test perimeter router and firewall devices at an industry standard frequency for vulnerabilities using industry standard testing methods. The Credentials will never be accessible on an Internet-visible computer. If Operator detects an intruder on an Operator networking or computer system, Operator shall disconnect the intruder immediately. Operators shall promptly report in writing to smartCommunicator any security deficiencies discovered by Operator as a result of such testing, or as a result of logging access attempts, along with Operator's action plan for curing such security deficiencies as soon as possible, but in no event more than ten (10) days after the date of its discovery.

Password and User Name Encryption

Operators shall encrypt the password and username files for their networks, databases, and computer systems using industry standard encryption. Any smartCommunicator credentials, passwords, or other information needed to operate the smartCommunicator Credentials will be stored on a server which is not visible to the Internet and with industry standard encryption.

(iv) Credentials. The credentials provided to Operators shall be carefully safeguarded and not distributed or shared with any unauthorized individual.

(vi) Maintenance. All networking, software, and computer systems must be maintained in good working order pursuant to hardware maintenance support available from trusted, reputable maintenance organizations.

(f) Security of Physical Premises. Operator shall limit access to its facilities to employees and employee-accompanied visitors using industry standard physical security methods. At a minimum, such methods must include visitor sign-ins, restricted access key cards or locks for employees, limited access to server rooms and archival backups, and burglar/intrusion alarm systems.

(g) training program in information security and in the protection of information resources for all personnel of Operator whose duties bring them into contact with the Imprinter.

(h) Confidentiality Agreements; Use of Contractors and Subcontractors. Operator shall cause all contractors, subcontractors, agents, and other persons or entities performing any part of Operator's responsibilities on behalf of Operator to comply with all the terms and conditions of this Security Policy.

(i) Security Audits. smartCommunicator will have the right, at its own expense, to inspect and audit, or to have an independent third party inspect and audit Operator's security measures and its compliance with this Security Policy. Operators shall (at their own expense) correct any security flaws detected by such an audit as soon as practicable. Operators will then promptly certify to smartCommunicator in writing that the security flaw has been corrected, along with a description of the corrective action(s) taken. All audits will be subject to the following conditions: (i) smartCommunicator must provide fourteen (14) days' notice before such an audit and may conduct no more than one audit annually; and (ii) any such inspection and audit must be conducted during regular business hours in such a manner as not to interfere with normal business activities.

10. Changes to Policies and Additional Requirements. smartCommunicator reserves the right to change or modify this Policy at any time. Good mail's Internet service or mailbox provider partners may also have their own requirements. Clients and Operators will be notified of changes within the smartCommunicator. Clients and Operators shall confirm their assent to any such new Policy within two (2) weeks of the new Policy being made available to them. Client's or Operator's delay in providing such assent may result in the temporary suspension of smartCommunicator service privileges. smartCommunicator may from time to time provide a Client with a small list of seed names (i.e., no more than 5) for the purpose of monitoring Client's compliance with this Policy, and Client shall include such seed names in its smartCommunicator service mailings.