Hillsong Internet and Email Usage Policy

UK

Date: June 2018
Updated: 28th December 2018

Introduction

This policy describes the rules governing internet and email use at Hillsong Church London ("Hillsong"). It also sets out the expected behavior when using the internet and email. It should be read alongside other key policies, in particular the **Hillsong Privacy Policy** (hillsong.com/privacy) and the **Hillsong Communications Policy**.

Purpose

It is important that every person at Hillsong who uses the internet and email understands how to do so responsibly, safely and legally. This Policy covers topics such as privacy, confidentiality, and security; ensures that electronic communications resources are used for appropriate purposes; informs employees regarding the applicability of laws and Hillsong policies to electronic communications; and prevents disruptions due to a misuse of Hillsong communications resources, services, and activity.

Policy Scope

This Policy applies to all full-time and part-time employees, contractors, volunteers and interns who use the internet and email (herein all referred to as "**the Individual**"). It applies no matter where that email or internet access takes place: on Hillsong premises, while travelling for Hillsong related activities or while working from home.

It applies to use of Hillsong email on any device, no matter whether owned by Hillsong or the Individual. It applies to use of the internet of any device that is owned by Hillsong, or that is connected to any Hillsong networks or systems.

Copyrighted Information

Individual must not use Hillsong's equipment, software, internet connection or email system to perform any tasks which may involve breach of copyright law.

Hillsong respects and operates within copyright laws. Individuals may not use the internet or email to:

- publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party;
- download illegal copies of music, films, games or other software, whether via file sharing services or other technologies.

Individuals should keep in mind that the copyright on letters, files and other documents attached to emails may be owned by the email sender, or by a third party. Forwarding such emails on to other people may breach this copyright.

Confidential Information

The leaking, theft or inadvertent release of confidential information represents one of the greatest dangers any business faces when permitting internet access to Individuals.

Confidential information should only be accessed or shared among authorized people, whether internal or external.

When sharing this data secure methods such as encryption and permissions should be used. Individuals must never email confidential data or ship it to someone on an unsecured USB flash drive.

Confidential data must be secured while “at rest.” Standard physical and digital access controls include file servers behind locked doors with access provided only to appropriate personnel.

Monitoring Internet and Email Use

Hillsong reserves the right to monitor use of the internet, to examine systems and review the data stored in those systems, and to monitor Individuals’ use of email.

Any such examinations or monitoring will only be carried out by authorised staff.

All internet data written, sent or received through Hillsong’s computer systems, and all emails sent or received through Hillsong’s email system, are part of official Hillsong records. Hillsong can be legally compelled to show that information to law enforcement agencies or other parties.

Individuals should always ensure that the information sent over or uploaded to the internet or sent via email is accurate, appropriate, ethical and legal.

Internet Use

Hillsong provides internet access as required for the performance and fulfilment of job responsibilities.

Occasional and reasonable personal use of Hillsong’s internet services is permitted, provided that the personal use does not interfere with work performance.

All rules described in this policy apply equally to personal internet use.

Personal internet use must not affect the internet service available to other people in Hillsong. For instance, downloading large files could slow access for other Individuals.

Individuals should not assume any guarantee of privacy if accessing the internet via Hillsong systems and should expect to be subject to monitoring and review.

Viewing or distributing inappropriate content is not acceptable under any circumstances. Individuals must not use Hillsong internet services to:

- take part in any activities on the internet that could bring Hillsong into disrepute;
- create or transmit material that might be defamatory or incur liability for Hillsong;
- disclose corporate information without prior authorisation;
- view, download, create or distribute any inappropriate content or material, including material that includes sexually explicit content or other material using vulgar, sexist, racist, threatening, violent or defamatory language;
- gamble, run secondary businesses, or engaging in “hacking” or other illegal activities;

- broadcast unsolicited personal views on social, political, religious or other non-business related matters.

All Individuals who access the internet should keep in mind they are representatives of Hillsong, whether in person or online.

Safe Internet Browsing

Individuals should only access sites known to be reliable. If in doubt, users can Google the site name to see if it appears to provoke security or malware concerns (check for negative reviews or reports of the site, warnings from security agencies, etc.).

Financial transactions conducted on Hillsong's behalf should be performed only by authorized personnel and via known good sites using https encryption.

Browser warnings can be cumbersome, particularly when trying to perform urgent tasks, but all Individuals are responsible for paying attention to these and adhering to the content.

If digital certificates used for encryption are suspicious, most browsers will inform viewers as such. Individuals must view the certificate information to see if it matches the site and whether it has expired, been revoked, or is in some other state.

Only plug-ins and extensions which are approved by the IT department should be installed within browsers on Hillsong machines.

The IT department is responsible for overseeing software updates including the latest browser versions. Individuals should never downgrade browsers or components such as plug-ins for security reasons.

Email Use

All @hillsong.co.uk or @volunteer.hillsong.co.uk must only be used for Hillsong-related business or activities.

Only people who have been authorised to use email at **Hillsong** may do so.

Personal use of the Hillsong's e-mail services is not encouraged, since there are a number of free alternatives available (Gmail, Yahoo, etc.). Individuals are urged to keep business and personal email separate.

Use of personal email during work hours should be of a reasonable level. All rules described in this Policy apply equally to personal email use and business email use.

Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered Hillsong property and are not the property of users of the electronic communications services. On ending a role at Hillsong, Individuals shall not be permitted to take any stored e-mails, calendar appointments or contacts with them.

Individuals may send and receive e-mail attachments that do not exceed 10 MB in size, provided that all attachments are scanned and confirmed to be virus free (using the Symantec antivirus application) before being sent or opened.

Individuals may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. Hillsong is committed to respecting the rights of the Individual, including the reasonable expectation of privacy. Recognising that some information is intended for specific

individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages.

Email Footers

Emails from Hillsong employee email accounts must include the following footer:

Hillsong Church London is a not-for-profit company limited by guarantee and registered in England and Wales. Company No: 05487537. Charity No: 1120355.

Registered office: 425 New Kings Road, London, SW6 4RN

Email confidentiality notice: This message is private and confidential. If you have received this message in error, please notify us and remove it from your system. If you are not the intended recipient, you must not copy, distribute or take any action in reference to it. Any such action may be unlawful.

Emails from Hillsong volunteer email accounts must include the following footer:

Hillsong Church London is a not-for-profit company limited by guarantee and registered in England and Wales. Company No: 05487537. Charity No: 1120355.

Registered office: 425 New Kings Road, London, SW6 4RN

Email confidentiality notice: Any views or opinions expressed are solely those of the author and do not necessarily represent those of Hillsong. This message is private and confidential. If you have received this message in error, please notify us and remove it from your system. If you are not the intended recipient, you must not copy, distribute or take any action in reference to it. Any such action may be unlawful.

Email Security

Users of the Hillsong email system must not:

- open email attachemtns from unknown sources, in case they contain a virus, Trojan, spyware or other malware;
- disable security or email scanning software. These tools are essential to protect Hillsong from security problems;
- send confidential company data via email. The IT department can advise on appropriate tools to use instead;
- access another Individual's Hillsong email account. If access to a specific message is required (for instance, while an Individual is off sick), they should approach the IT department;
- click on suspicious links in email messages; if the mouse cursor is hovered over the link, this will often reveal the true address;
- never respond to spam/unsolicited offers from strangers such as alleged Nigerian princes, deposed dictators or other individuals promising to share a fortune for an upfront fee (the sender will invariably disappear after their targets pay, without further communication). When it comes to these types of offers, "if it sounds too good to be true, it is!"

Individuals must always consider the security of Hillsong's systems and data when using email. If required, help and guidance is available from the IT department.

Individuals should note that email is not inherently secure. Most emails transmitted over the internet are sent in plain text. This means they are vulnerable to interception. Although such

interceptions are rare, email should be regarded as an open communication system, not suitable for confidential messages and information.

Inappropriate Email Content and Use

Hillsong email must not be used to send or store inappropriate content or materials.

Viewing or distributing inappropriate content via email is not acceptable under any circumstances.

Individuals must not:

- Write or send emails that might be defamatory or incur liability for Hillsong;
- Create or distribute any inappropriate content or material via email, including material that includes sexually explicit content or other material using vulgar, sexist, racist, threatening, violent or defamatory language;
- Send messages or material that could damage Hillsong's image or reputation.

Any Individual who receives an email they consider to be inappropriate should report this to their Department Leader.

Blanket forwarding of messages to parties outside Hillsong, and the mass distribution of unsolicited e-mail messages, is prohibited.

Contracts and Liability

Individuals must be careful about making commitments or agreeing to purchases via email.

An email message may form a legally binding contract between Hillsong and the recipient – even if the Individual has not obtained proper authorisation.

General Usage Guidelines

General usage guidelines are intended to fill in any gaps which the prior requirements may have left out.

Insecure public wireless networks are one of the most prevalent methods in which passwords and data can be captured by malicious individuals; these should never be used. If there is no alternative, a VPN connection should be made over said wireless network to the Hillsong network (split tunneling disabled) to protect network traffic.

Individuals' devices should not be left attended without activating a screen lock. Portable devices should be kept secure at all times, especially when travelling.

Never write or save passwords as these could be used if the device is compromised by another individual.

Regardless of the circumstances, individual passwords must never be shared or revealed to anyone. To do so exposes the Individual to responsibility for actions the other party takes with the password. If a password must be provided (such as to a new user working remotely) do so over the phone so their identity can be confirmed.

Individuals should never tamper with security software or functions which are intended to protect devices.

Report anything out of the ordinary to the IT department for analysis and investigation.

Data Protection

Individuals must not share, link to, use or store any information in a way that would breach Hillsong's Privacy Policy (hillsong.com/privacy).

Where a deletion request has been made by an individual, all records involving that person must be permanently deleted and all email correspondence with that individual and the email address itself must be deleted, with the exception of the record held by the Hillsong Data Protection Office.

Violations and Penalties

Violations of this Policy could result in disciplinary action including termination of employment. Users may also be held personally liable for violating this Policy.

Where appropriate, Hillsong will involve the police or other law enforcement agencies in relation to breaches of this Policy.

Any violation of this Policy must be immediately reported to any relevant Department Leader, the IT and the Human Resources departments, and to the Hillsong Data Protection Officer.

Contacts

Hillsong Church London

0207 384 9200

Data Protection Officer

dataprotection@hillsong.co.uk

Hillsong IT Department

IT@hillsong.co.uk