Email Policy

Last updated Feb 2024

Name of Document	PCUK Email Policy
Document Version	Version 1.0
Author	PCUK
Approved by	PCUK Board of Trustees
Type	Policy
Date Approved	16th February 2024
Last reviewed	
Review frequency	Biannually
Next Review	16th February 2026

Version History		
Version	**Date**	**Description**
1.00	02.2024	Original Document

Contents

Policy brief & purpose

Our corporate email usage policy helps Police Chaplaincy UK Trustees / Board members to use their corporate email addresses appropriately. Email is essential to roles as Trustees / Board members of Police Chaplaincy UK. We want to ensure that our Trustees / Board members understand the limitations of using their corporate email accounts.

Our goal is to protect our confidential data from breaches and safeguard our reputation and technological property.

Scope

This policy applies to all Trustees / Board members, employees and partners who are assigned (or given access to) a corporate email. This email may be assigned to an individual (e.g. name@policechaplaincy.uk) or role (e.g. secretary@policechaplaincy.uk.)

Policy elements

Corporate emails are powerful tools that help Police Chaplaincy UK Trustees / Board members in their roles. Trustees / Board members should use their corporate email primarily for Police Chaplaincy UK purposes. However, we want to provide some freedom to use emails for personal reasons.

We will define what constitutes appropriate and inappropriate use.

Inappropriate use of corporate email

Our Trustees / Board members represent Police Chaplaincy UK whenever they use their corporate email address. They must not:

- Sign up for illegal, unreliable, disreputable or suspect websites and services.
- Send unauthorised marketing content or solicitation emails.
- Send insulting or discriminatory messages and content.
- Intentionally spam other people’s emails.

Police Chaplaincy UK has the right to monitor and archive corporate emails and may access corporate email accounts from time to time for technical updates.

Appropriate use of corporate email

Trustees / Board members are allowed to use their corporate email for work-related purposes without limitations. For example, they can use their email to:

- Communicate with current or prospective members and partners.
- Log in to purchased software they have legitimate access to.
- Give their email address to people they meet at conferences, career fairs or other corporate events for business purposes.
- Sign up for newsletters, platforms and other online services that will help them with their roles or professional growth.

Trustees / Board members should use CC & BCC with care.

Every time a message containing personal data is copied to another recipient there is an increased information compliance risk.

To minimise risk, we make the following recommendations:

- Limit the use of CC only to those who need to receive the information.
- Where you regularly have to send personal information, use alternative sharing tools such as Dropbox and OneDrive.
- With the above in mind where it is still necessary to send to multiple recipients, BCC (Blind Carbon Copy) can be a useful tool. BCC is a means of sending an email to a large number of people without them knowing who else is getting the email.

Personal use

Trustees / Board members are allowed to use their corporate email for some personal reasons. For example, they can use their corporate email to:

- Register for conferences or gatherings.
- Send emails to friends and family as long as they don't spam or disclose confidential information.
- Download ebooks, guides and other content for their personal use as long as it is safe and appropriate.

Trustees / Board members must adhere to this policy at all times.

Email security

Email is often the medium of hacker attacks, confidentiality breaches, viruses and other malware. These issues can compromise our reputation, legality and security of our equipment.

Police Chaplaincy UK will select strong passwords for the corporate accounts and keep a record of them securely. As corporate emails are only given to board members during their term of office Police Chaplaincy UK will take responsibility for issuing and changing passwords rather than individuals.

Trustees / Board members should always be vigilant to catch emails that carry malware or phishing attempts. We instruct employees to:

- Avoid opening attachments and clicking on links when content is not adequately explained (e.g. "Watch this video, it's amazing.")
- Be suspicious of clickbait titles.

- Check email and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

We remind our Trustees / Board members to keep their anti-malware programs updated.

Email signature

We encourage Trustees / Board members to create an email signature that exudes professionalism and represents Police Chaplaincy UK well.

Here's a template of an acceptable email signature:

[Trustees / Board members Name]

[Title], [Company Name]

[Phone number] | [Website & Twitter Address]

Trustees / Board members may also include professional images, logos and work-related videos and links in email signatures.

A confidentially notice will be added to all email signatures by Police Chaplaincy UK, this will state

This email contains information which is confidential and may also be privileged. It is for the exclusive use of the addressee(s) and any views or opinions expressed within are those of the originator and not necessarily those of Police Chaplaincy UK. If you are not the intended recipient(s) please note that any form of distribution, copying or use of this email or the information contained is strictly prohibited and may be unlawful. If you have received this communication in error please forward a copy to admin@policechaplaincy.uk and to the sender. Please then delete the email and destroy any copies of it. DO NOT use this email address for other enquiries as it will not be responded to, nor any action taken upon it. Police Chaplaincy UK is not a police force, if you need to contact the police please ring 101. If it is an emergency, please call 999. Thank you.

Disciplinary action

Trustees / Board members who don't adhere to the present policy may face disciplinary action up to and including dismissal. Any disciplinary action will be referred to the Trustees / Board members own Force's Professional Standards Department.

Example reasons for referral to PSD action are:

- Using a corporate email address to send confidential data without authorisation.
- Sending offensive or inappropriate emails
- Using a corporate email for an illegal activity.

The Police Chaplaincy UK Communications officer takes responsibility for corporate email addresses and can be contacted at comms@policechaplaincy.uk

Feb 2024