Pearson Ham Group Digital Security Policy Statement

July 2024

Introduction

At Pearson Ham Group, we are strongly committed to upholding the highest standards of information security and privacy. We recognise that we may handle proprietary, sensitive, or otherwise protected information, including clients' business priorities, personal information, and trade secrets. Confidentiality is crucial to Pearson Ham Group and its clients, colleagues, expert networks, applicants, and business partners.

All Pearson Ham Group employees, affiliates, and third parties acting on behalf of Pearson Ham Group, universally across all Pearson Ham Group office locations, must protect confidential information from unauthorised disclosure, use, and loss. This includes respecting ethical walls and ensuring that client data and internal material remain within authorized repositories. Pearson Ham Group signs suitable confidentiality agreements with its clients and prospective clients, ensuring that the confidentiality of their data and the work we do for them is maintained.

Information Security and Privacy

All Pearson Ham Group employees commit to protecting information security and privacy across all stages of engagements with our clients. Guidelines and training are provided on how to safely transmit, handle, store, and delete unnecessary data.

In accordance with our obligations regarding Privacy and Personal Data Protection, Pearson Ham Group follows GDPR regulations. This extends to all employees, affiliates, and third parties acting on behalf of Pearson Ham Group. Additionally, we comply with other relevant data protection laws applicable to our operations globally.

Use of Information Assets

Pearson Ham Group has rigorous internal policies that govern the responsible and ethical use of information assets. The term "information assets" applies to information systems and other information/equipment, including paper documents, mobile phones, portable computers, data storage media, etc., which are owned or used by Pearson Ham Group, or which are under Pearson Ham Group's responsibility.

Examples of prohibited use of information assets include:

- Illegal activities
- Accessing, downloading, or distributing inappropriate or offensive content
- Installing software not authorised by the PHG IT Council

Equipment, information, or software, regardless of its form or storage medium, may only be taken off-site for the purposes of remote working. All other cases require written permission from an HR & Operations Manager. Pearson Ham Group employees must commit to taking privacy and safety precautions, including, but not limited to:

- Only using secure WiFi connections
- Not displaying sensitive data on screens in public locations
- Not leaving devices unlocked when not in use

All Pearson Ham Group employees should apply good security practices when selecting and using passwords, as described in internal policies.

All owned Pearson Ham Group software systems must have malware-protection measures installed and regularly maintained.

Compliance and Reporting

Pearson Ham Group has an PHG IT Council responsible for supporting compliance with the policies. The IT team commits to reviewing these policies at least annually to ensure we continuously operate with the highest standards and adapt to evolving risks to digital security and privacy.

Suspected policy violations, legal or regulatory breaches, or ethical breaches should be reported to the Pearson Ham Group CEO and/or HR at susiecanny@pearsonhamgroup.com. We take all reports seriously and will investigate promptly, taking appropriate action to mitigate any identified risks.