



Workhuman Acceptable Use Policy

To allow you to fully participate in the workplace and facilitate you in carrying out your role, Workhuman will provide you with IT Services, including but not limited to IT equipment, access to systems, services, and applications, including, but not limited to e-mail, learning systems, SaaS services, etc. To protect you, your colleagues, and Workhuman, we all need to utilise all applications and services in an acceptable manner consistent with this policy. Failure to do so may result in disciplinary action, up to and including dismissal.

This policy applies to the following: Workhuman employees, contractors, consultants, temporary staff, and all other workers accessing Workhuman's IT Services, including all personnel affiliated with third parties.

All IT Services are the property of Workhuman and are provided for conducting Workhuman's business. A certain amount of personal use is acceptable, provided it is consistent with this policy, is not excessive, and does not interfere with Workhuman's business or damage Workhuman's reputation.

You can have no expectation of privacy when using Workhuman IT Services. Workhuman, as it may deem appropriate, reserves the right at all times to access, monitor, review, copy, or delete any information stored or transmitted on any of Workhuman's IT Services.

You are expected to utilise good judgement in all uses of Workhuman's IT Services.

The following activities are directly forbidden on Workhuman IT Services:

- Any activity that is illegal under national, federal, state, local, or international law.
- Unauthorized sharing of Workhuman Private or Workhuman Confidential Internal information including the personal information of any individual. Taking screenshots of photos of screens with such information is forbidden.
- Viewing, sharing, or storing obscene, pornographic, abusive, slanderous, defamatory, harassing, vulgar, threatening, and other offensive material. Offensive material includes, but is not limited to, any material which disparages another person based on gender, sexual orientation, race, colour, national origin, religious beliefs, marital status, family status, age or disability. In all such cases, the potential impact on the recipient determines whether material is offensive.
- Sending to/from or uploading Workhuman's Workhuman Private or Workhuman Confidential - Internal data to personal e-mail addresses or internet storage applications, including but not limited to Gmail, iCloud, Outlook.com, Google Drive, or Dropbox.
- Install or utilise any tool or technology outside the scope of your job role that monitors, listens, scans, sniffs, or interferes with any of Workhuman's IT Services.
- Bypassing or attempting to bypass any IT security controls.
- Copying or distributing copyrighted materials in violation of copyright laws.
- Unauthorized use of Workhuman's name, logo, trademarks, or other intellectual property.



- Actions that violate any other Workhuman policies including those addressing confidentiality, non-solicitation, and harassment.
- Using Workhuman's IT Services and equipment to conduct business on behalf of third parties, including side businesses and freelance work.

You should always observe these acceptable use practices:

- Keep your passwords secure and do not share accounts. You are responsible for all actions which take place under your assigned logon. Set strong passwords and do not set the same password for your personal IT services as you do for accessing Workhuman's IT Services.
- Ensure that all software and IT services you use are authorised through Workhuman's IT governance process.
- Complete all assigned IT Security Awareness training promptly and openly.
- When authorised to share Workhuman Private or Workhuman Confidential Internal information as part of your job role, you must use appropriate security measures including encryption. If in doubt, ask your manager or Information Security to discuss these measures.
- When accessing Workhuman's IT services remotely, set up your home network / Wi-Fi in line with your service provider's instructions and best practices. In using unsecured, public Wi-Fi always confirm the identity of the Wi-Fi access point and use VPN where possible.
- Lock your screen when you leave your work area – every time.
- Keep Workhuman's IT equipment safe and secure, whether in our offices or visiting customers, working remotely, when attending events, and when travelling.
- Do not allow unauthorised persons to utilise Workhuman's IT Services and equipment.
- Return all IT equipment and cease using any Workhuman IT Services at the end of your employment or when requested to do so by Workhuman.
- Protect confidential files and papers when working with them. Lock items in a drawer if you need to leave the area and dispose of items securely when finished working with them. Limit printing and never print personal data.
- Report loss of equipment to the Workhuman Helpdesk and Information Security as soon as possible.

Information security is the protection of the Confidentiality, Integrity and Availability of information. **Information Security is the responsibility of every person who is granted access to Workhuman's IT Services.** Further information is available in the Workhuman Information Security Policy. Please report anything suspicious or that you believe may impact the security or data of Workhuman to Workhuman's Help Desk or to Infosec@workhuman.com.

Please refer to Workhuman's Bring Your Own Device (BYOD) policy for additional guidance relating to use of Workhuman's IT services from your personal IT devices. Please refer to Workhuman's Social Media Policy for additional guidance relating to acceptable conduct on social media platforms.