Our Commitment to Security & Privacy: A Guide for Our Team

Last reviewed: 05.01.2025

At Honch, even with our small team, protecting our information and our clients' privacy is a top priority. This short guide outlines our key principles and essential practices. Remember, **security and privacy are everyone's responsibility**, and your vigilance is our strongest defense.

Why It Matters to Us

- **Protecting Our Business:** A single security slip-up can impact our operations, reputation, and financial stability. Your awareness helps keep us running smoothly.
- **Safeguarding Our Clients:** While we don't handle sensitive information, upholding privacy builds trust and is fundamental to our client relationships.
- **Your Role is Crucial:** Technical safeguards are important, but human error is the leading cause of breaches. You are our first and most important line of defence.

Key Principles & Practices

We don't just "train" once; we maintain a continuous dialogue about these critical areas:

1. Spotting & Avoiding Threats (Phishing & Social Engineering)

Cybercriminals are clever. They'll try to trick you into revealing information or clicking malicious links.

- **Always Be Sceptical:** Treat unexpected emails, texts, or calls with caution, even if they seem to come from a trusted source.
- **Look for Red Flags:** Misspellings, urgent language, generic greetings, and suspicious links are common signs of phishing.
- **Verify, Don't Click:** If something feels off, independently verify the sender. Call them directly using a known number (not one from the suspicious message).
- **Never Share Credentials:** No legitimate organisation will ask you for your password or other sensitive login details via email or text.

2. Strong Passwords & Account Security

Your passwords are the keys to our digital assets. Treat them like gold.

- **Make Them Unique:** Use a different, strong password for every account. Don't reuse passwords, especially for work-related tools.
- **Aim for Complexity:** Use a mix of uppercase and lowercase letters, numbers, and symbols. The longer, the better.
- **Enforced Multi-Factor Authentication (MFA/2FA):** We always turn on MFA. This adds an extra layer of security making it much harder for unauthorised access.

3. Secure Handling of Information

Whether it's client data or our own internal files, how we handle information directly impacts our security.

- **"Need to Know" Access:** Only access information necessary for your role.
- **Secure File Sharing:** Only use company approved, secure methods for sharing sensitive documents. Avoid personal cloud services or unencrypted email attachments for confidential data.
- **Clean Desk Policy:** Don't leave sensitive documents or devices unattended and unlocked. Shred or securely dispose of confidential paper waste.
- **Secure Devices:** Always lock your computer or device when stepping away, even for a moment.
- **Public Wi-Fi Warning:** Avoid accessing sensitive company information over unsecured public Wi-Fi networks.

4. What to Do If Something Feels Wrong

You are our eyes and ears. If you suspect an issue, don't hesitate.

- **Don't Panic, Don't Delete:** If you suspect a phishing email or a security incident, don't delete it. Immediately forward this to London Systems at helpdesk@lonsys.co.uk
- **Report Immediately:** Inform Anthony Cooper or Emma Evans right away. Even small concerns can prevent big problems.
- **When in Doubt, Ask!** It's always better to ask a question than to make a mistake.

Thank you for your ongoing commitment to keeping Honch secure and our clients' privacy protected. Your awareness and actions make all the difference!