Safety Hour Discussion Pack

Topic: Secure use of devices

Ask yourself, do you know what 'acceptable use' is?

Purpose of the discussion:

To discuss what acceptable use is and how it applies to our security at home and at work.

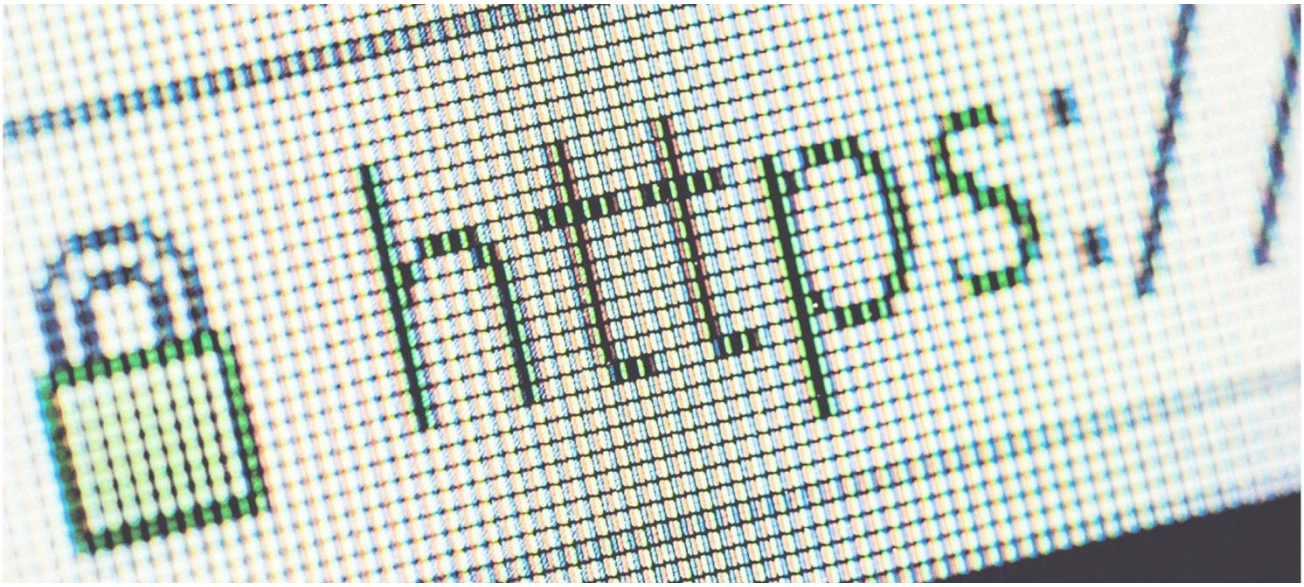
Before the session, if you haven't already done so, complete the mandatory security training via Oracle ebusiness OLM by searching for 'information security'. This will give you more information and help you to answer questions raised during the discussion.

Kick-off the discussion:

Start the discussion by saying –

What do you think '**acceptable use of Network Rail information and information systems'** means? This is a standard that we all agree to, as part of our terms and conditions of employment. But how many of us have read it, or even heard of it?

This Safety Hour is part of a series based around 8 questions we should ask ourselves in order to work securely and understand the contents of our security policy and standards. We want to avoid security breaches or incidents which could impact the safe operation of the railway and the safety of our colleagues and customers.
Find out more about the 8 asks here: http://oc.hiav.networkrail.co.uk/SITES/SEC_CHAMPS/



home safe plan

Safety Hour Discussion Pack

Topic: Secure use of devices

Ask yourself, do you know what 'acceptable use' is?

Discussion points: Use below to plan your facilitated discussion. Remember, you don't have to have all the answers – the role of the facilitator is to create an engaging discussion where everyone identifies and commits to solutions.

Discussion points	Supporting notes
Why is the 'acceptable use' standard important for the safety of our railway? **Find the acceptable use standard on Connect by clicking this link or asking your line manager to print out a copy**	The standard covers different aspects of use of our devices and systems for different reasons. It helps us to: • Keep our systems secure • Protect ourselves and our information • Protect the company's reputation You are responsible for your use of devices, websites you visit, content you publish online, controlling access and keeping devices secure. **How could insecure or inappropriate use of our devices impact safety?** Our railway increasingly relies on digital systems and equipment, if they are compromised either intentionally or accidentally what might the consequences be? **The potentially unsafe circumstances that could be caused by misuse of our systems are many and varied and the threat and risks are developing and changing all the time. Secure and responsible use of our systems and equipment is everyone's responsibility. Remain vigilant and report incidents or raise concerns via Close Call.** **Key messages here are:** • **Consider security when using Network Rail systems, think of the impact of your actions and decisions** • **If you have security concerns, Close Call them or speak to asksecurity@networkrail.co.uk**

Safety Hour Discussion Pack

Topic: Secure use of devices

Ask yourself, do you know what 'acceptable use' is?

Discussion points: Use below to plan your facilitated discussion. Remember, you don't have to have all the answers – the role of the facilitator is to create an engaging discussion where everyone identifies and commits to solutions.

Discussion points	Supporting notes
Acceptable use involves considering security in the way we all use technology. Use the questions below to start a discussion about how 'acceptable use…' might impact safety and security. We don't expect anyone to have all the answer to these questions, the point is we all play a part in creating a safe railway and preventing security breaches.	• How do we control access to our systems and information? Do our team only have access to systems and information they need to do their role? What could happen if everyone had access to our systems and information? Who might want to gain access in order to create an unsafe situation? • What part do passwords play in controlling access? Are we good at making strong passwords? Do we make weak passwords, thinking it won't happen to us? Do we share passwords? (If shared passwords are in practice, are they limited to those that need to know, within a closed group?) • What about how we connect our devices? How do you know connections are secure? What are the risks personally and professionally? Why are we targeted? How could a breach or attack affect safety? • What if our devices or equipment got into the wrong hands, a malicious person who intends to damage or misuse our systems or information? **Key messages** • **Only authorised staff should access our systems, access should be controlled.** • **Think about your password and find a method for creating unique and strong passwords. Don't leave an open door for cyber criminals, see Safety Hour – Secure passwords for more information.** • **Consider the risks of using different connections, for more information see Safety Hour – Secure connections.** • **Keep your devices secure at work, when travelling, in public and at home. Our devices are valuable not just financially but for the systems and information they can connect to.**

Safety Hour Discussion Pack

Topic: Secure use of devices

Ask yourself, do you know what 'acceptable use' is?

Discussion points: Use below to plan your facilitated discussion. Remember, you don't have to have all the answers – the role of the facilitator is to create an engaging discussion where everyone identifies and commits to solutions.

Discussion points	Supporting notes
What do we need to do?	• What percentage of our emails are blocked everyday? 80% with roughly 1000 medium and high risk attacks intercepted daily! Some things do get through our filters and it only takes one person to open an email to infect our files. Has anyone been a victim of a malicious email? What were the consequences? Were you affected financially? • Has anyone been fooled by a fake website? Did it affect your devices? Steal your money? Cause you stress and worry? Were you targeted specifically? • Do you think about what you post on social media? What might be the risk of posting a picture or update identifying you as a Network Rail employee? Why might posting a picture of you in work pose a security risk? **Key messages here are:** • **Know how to spot a suspicious email, if you receive something that doesn't look right, don't open it and make sure you send it as an attachment to spammail@networkrail.co.uk to make sure.** • **Understand the risks of spoof websites and look for the signs of a trusted site, HTTPs etc. If in doubt type the known address in the browser instead of following a link.** • **Be careful when posting online, check your privacy settings and consider the importance of your role and where you work, we are critical national infrastructure.** • **Remain vigilant and challenge unacceptable use of our systems and devices – close call security concerns.** • **For more information on any of these subjects search for 'Security' on Connect or email asksecurity@networkrail.co.uk**

Safety hour based on one of the 8 Ask Yourself security questions.
Select those most relevant to you and if you have any questions or concerns about security or delivering this safety hour please get in touch.
Contact AskSecurity@networkrail.co.uk or search 'Security' on connect.
Use #AskSecurity to visit the Information Security group on Yammer.

home safe plan