Stanley School

Security Policy – Dos and Don’ts

Do read and familiarise yourself with this policy

All staff and pupils with access to ICT facilities are bound by the requirements in that policy. It is your responsibility to familiarise yourself with the contents.

Don’t share your username and password

Under no circumstances should your username and password be used by someone else to log on to the network. If you share your login details any inappropriate activity on your account will be recorded against you. If you think someone else knows your password, contact your IT support and have it reset.

- If you or a colleague needs access to an IT system, **apply for it**
- And, most importantly, **do not log on to someone else's account**

Do use complex passwords and keep them safe

Your User ID and password are the first line of defence for the School’s ICT systems. Choose a ‘strong’ or complex password to minimise others being able to access your account.

- Your password should have at least seven characters and include upper and lower case.
- Avoid using a password that could easily be guessed such as names, telephone numbers and dates of birth.
- Don’t put the password on a post it note, if you need to write it down then keep it secure.

Do adhere to the clear desk policy

- Do familiarise yourself with the clear desk policy, it gives tips for school based and home working.

Do use the 'locked print' function

If you don’t currently have locked prints then ask your IT technician to set it up for you.

Do lock your computer when leaving it unattended

When leaving a computer unattended even for a short time, the screen must be ‘locked’ to prevent others accessing your account. Simply press ‘Ctrl, Alt, Delete’ at the same time and select ‘Lock Computer’. On your return the computer will prompt you for your log in details before allowing access to the desktop screen.

Don't leave documents on printers/faxes/copiers

Once you have printed your document, sent a fax or made a copy of it keep it stored securely to avoid an information security incident.

Do report suspected information and ICT incidents

Any event that may compromise the confidentiality, availability or integrity of School information is an information or security incident. This includes disclosure of information to someone not authorised as well as the loss of, or damage to ICT equipment that stores or processes School information.

You need to report any such incidents to your DPO so that they can help you decide if any action needs to be taken and help you reduce the possibility of similar events occurring.

The DPO may ask you to complete a data breach form.

Do escort visitors to and from reception and challenge any visitors with no identification badge/contractors pass or who have not signed into your school

Be aware of who is in your building and raise any queries with staff who are on reception duty.

Those who require access will have a security pass or those who are visitors will be given appropriate access.

Email

Don’t misuse the School’s email facilities

Non-compliance with any school ICT policies may result in disciplinary action. The forwarding of emails from a school secure email address to a personal email account (for example to work at home) if any personal data is contained in the email. The forwarding of so-called chain emails, including joke emails, is also prohibited as they use network and storage space and may contain viruses.

Do send sensitive or personal data by secure means

Personal or sensitive School information could include:

Personal information relating to individuals, particularly children,

- Financial or commercially sensitive information,
- Information which could negatively affect the School if disclosed to unauthorised individuals or organisations
- Personal or sensitive information must never be sent by fax.

Don't respond to suspicious emails

Spam is the name given to bulk emails sent to a random selection of email addresses. Spam is mainly 'phishing' emails which attempt to obtain personal information such as bank details and 'pharming' emails which try to get users to click on web links to often malicious websites.

The School has introduced measures prevent the majority of Spam emails getting to users' accounts. Unfortunately the senders of these emails continue to find way of bypassing controls.

If you suspect an email is Spam, or looks suspicious in nature, **DELETE IT IMMEDIATELY and DO NOT REPLY.**

Storage

Don't use personal devices to connect to School network or store School Information unless they conform to the Bring Your Own Device Policy

Check the BYOD policy before connecting personal equipment to School computers or the network as this could inadvertently introduce malware, such as viruses onto the network. Personal devices are those that are not issued by the School and include, but are not limited to:

- Laptops
- Tablet PCs
- Mobile phones
- PDAs
- MP3 players
- Data/Memory sticks

Don't store School information on insecure devices

Data stored on insecure devices (e.g.: unprotected removable media, laptops, tablet PCs) is at risk of being compromised if lost, stolen or damaged. Devices should be secured with 2 factor authentication, or encryption to prevent unauthorised access to any data held on them.

Do store and dispose of documents safely

The School operates a clear desk policy, familiarise yourself with this.

Here to help?

If you have questions or concerns you can ask your ICT technician or your software support officer or drop an email to Schoolsdpo@wirral.gov.uk