KINGSWAY PRIMARY SCHOOL
Security Policy – Dos and Don'ts
January 2021

Do read and familiarise yourself with this policy
All staff and pupils with access to ICT facilities are bound by the requirements in this 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 any device or 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'. 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.
Do not forward emails from a school email address to a personal email account (for example to work at home) if any personal data is contained in the email.
Do not forward chain emails, including joke emails, as they may contain viruses or other malware.

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

Ask your IT support for advice on how to send information securely.
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. 'Phishing' emails attempt to obtain personal information such as bank details or 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.** Inform your IT Support immediately if you have clicked on a link which you believe to be suspicious or malicious.

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
- Datasticks

Don't store School information on insecure devices

Data stored on, or accessed via, insecure devices (e.g.: removable media, laptops, tablet PCs) is at risk of being compromised if the device is lost, stolen or damaged. Removable or portable devices should be encrypted. Two factor authentication should be used to prevent unauthorised access to systems.

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

Advice on using Zoom video meetings in schools

Background

Some schools have asked for advice regarding the use of Zoom for classroom activities and I have asked the Council's IT Security Officer to put together some guidance/advice so you can make an informed decision to use Zoom or not. It's about being aware of how to safely use Zoom and to be aware of the risks involved and how to mitigate them.

Wirral Council's preferred video meeting application is Microsoft Teams which should be used whenever possible. If a school has access to the corporate Teams system it should use this to hold video meetings with parents, pupils etc.

Zoom has become an extremely popular video meeting tool since the start of the pandemic. It is easy to use and has lots of very useful features but can be "hacked" if the security settings are not configured or used correctly.
A key risk that needs to be understood and managed correctly is that an uninvited person could join a meeting and then share distressing videos/images with all participants. To prevent this you should carefully manage who joins the meeting and do not allow participants to share their desktop or files by default.

Do not publish the meeting details in a public place, for example the school website or twitter feed. You can publish the date, time, purpose etc but do not publish the link to the Zoom meeting or the meeting ID or password as these details can be used by uninvited participants. Instead, send the meeting invitation to each child or parent via a direct messaging system or email.

Preparation Before Using Zoom

Before the meeting

When setting up the meeting, make sure that the following features are enabled:

- Require meeting password. This setting is now on by default for all meetings.
- Disable "Enable join before host". This ensures that the host is the first person to join the meeting.
- Enable waiting room. This allows you to let people into the meeting one-by-one when you're ready. Also, the host can put people back in the waiting room during the meeting. For example, if there's any doubt about who they are.
- Set screen sharing to "host only". Participants will not be able to share their screen unless the host switches this on during the meeting.

During the meeting

- Use the Security tab to switch on or off other features like allowing participants to share their screen or to use Chat, and to Lock the meeting so that nobody else can join.
- Use the Participants list to Mute participants, to switch their video off, remove them from the meeting or move them to the Waiting Room.

Points to note

- The free version of Zoom currently limits meetings of 3 or more people to 40 minutes, although the meeting can then be restarted.
- Paid-for Zoom licences allow pre-registration of participants which further reduces the risk of uninvited attendees.
- Large meetings with lots of participants require management.
    - Inform the participants that you will be using a waiting room and that there will be a slight delay at the start of the meeting.
    - Make a colleague a Co-host and give them the responsibility of admitting people from the waiting room after checking their names.

Managing the Chat feature

Chat is a useful tool during meetings but is has some features which you may want to consider:

- The Host can configure whether Participants can chat with nobody, the Host only, Everyone publicly, or Everyone publicly and privately. You may choose to switch off private chat as a safeguarding protection if a child may be the unsupervised recipient of a chat private message.
- Chat also allows participants to share files with all attendees. This can be switched off, in advance of the meeting, by logging into the Zoom web client and going to Settings – Meeting - File Transfer - Hosts and participants can send files through the in-meeting chat.

Key points

- Do not overshare the Zoom meeting details.
- Use a Waiting Room.
- End the meeting immediately if you are not comfortable with the safety or security of the invited meeting participants.
- Hold a practice meeting with a small number of colleagues before holding a larger meeting so that you are familiar with all of the settings and controls.

Advice provided to be considered by Schools before using Zoom – January 2021

School Clear Desk Checklist for All Staff

Introduction

Even though much of our work is done electronically, using Internet, Cloud and Microsoft Teams, we also need to remember paper. Or "The Enemy" as I like to call it, many security breaches are paper based……so remember Post it notes and paper records which can be easily left on desks, printers, car roofs, parking meters, in shops. This list is aimed at being a quick reminder on how to keep information safe and yes it's common sense but it's worth a quick read.

At the end of the working day check you have:-

- Put your ICT equipment/phone in a locked and secure place if you are not taking it home.

- Cleared all paperwork containing personal or sensitive data from your desk/office or classroom and secured it or disposed of it. Please check for post it notes and scribbled reminders containing personal and sensitive information.
- Disposed of paper in the correct bin or rubbish sack - do not leave anything confidential or sensitive in a normal waste bin.
- Checked the printer and know you have collected or disposed of all your printing for that day.
- Put out of sight any keys for drawers/filing cabinets etc.

At the end of a meeting check you have…

- Removed and either destroyed or stored away any flip chart paper with personal or sensitive information on it.
- Erased any personal data from Whiteboards.
- Cleared, and disposed of any paperwork used during the meeting, which you no longer need.

Before taking work home ask yourself…

- Do you need to remove paper records from the school, could you work from home electronically rather than take physical papers?
- How are you transporting the paperwork home?

At home…

- The clear desk school guidelines apply to your home as well, as sometimes your home is indeed your workplace.
- During the day you should be mindful of leaving paperwork unattended / in view of others who may be in your home.
- Use Ctrl Alt Del keys to lock your machine if leaving it unattended, it's a great habit to get into.
- Don't share your passwords or ask others to remember them for you.

If you have any questions or queries then please contact me:-
Schoolsdpo@wirral.gov.uk
Via Microsoft Teams Call 0151 691 8645
Via Mobile 07768926323

Document reviewed January 2021
Next Review Date January 2023