Mapledown School
E-Safety

S M A R T

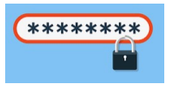
Set

different passwords for different areas of your online life.

It's tempting to set one password for everything. This makes life easier for you, but also makes it easier for others to steal personal information from you.

A strong password is longer than eight characters in length and includes a mix of upper and lowercase letters, numbers and special characters.

At school, we must log in and out every time we use a PC. We are responsible for the use of that PC whilst our school account is signed in. **Do not** share your password with anyone else or allow unauthorised individuals to access our school network. Contact ICT Support to request login accounts for staff or Wi-Fi access for visitors.



Monitor

our students carefully as they access the internet on school devices.

It is our duty to keep our pupils safe whilst using technology. Make sure that **online activity is appropriate** at all times, especially when pupils are navigating sites such as YouTube during leisure time.

To help keep our school community and your own family safe online, check the advice and information on these websites:

internet matters.org

NSPCC

childline

mumsnet

Always

watch out for phishing scams.

Phishing scams use fraudulent emails and websites to trick users into disclosing private account or login Information.

Only click on an email link if you are expecting it e.g. you've just ordered something from a company online or you've just signed up for an account on a website.

Never click on links or open attachments in unexpected emails, e.g. from your bank, energy supplier or even your friend. Contact them separately to find out if the email is genuine.

If you are asked to log into a website, go directly to the app or official site instead.

Report

any concerns about students' e-safety to the Leadership Team.

Remember that personal devices are **not allowed** to be used to take photos or videos of students.

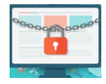
Mobile phones can be used in the staffroom, resources room, medical room, main school office or outside the front of the school. Mobile phones **may not** be used in any other area, **except in an emergency**, e.g. to call 999 for an ambulance or other emergency service.

Be informed of **parental permissions** concerning the publication and sharing of children's digital/ video images. Check with the school office for further guidance. **Never** assume consent.

Be aware of which students are allowed to be visible on camera during **remote learning** sessions.

Think

about what you say and do online.



Keep personal information personal. Lock down your privacy settings and avoid posting things like birthdays, addresses, mother's maiden name, etc.

Be wary of requests to connect from people you don't know. Block people who send nasty messages.

When connecting to **public Wi-Fi** networks, be cautious about what information you are sending over it. **Never** use public Wi-Fi to sign in to any app or website that contains your personal information.

When shopping or banking online, check the site's address. The address should always start with "https" instead of just "http" and have a padlock icon in the website address field.

Be on the lookout for websites that have misspellings or bad grammar in their addresses. They could be copycats of legitimate websites.