LIMPSFIELD GRANGE SCHOOL

'together we make a difference'

Procedures for staff accessing school email and other school information on handheld devices

Phones and other mobile devices often contain your personal information, such as email addresses and phone numbers. Even with the utmost care and attention it is very easy to lose mobile devices and the following security measures should be taken.

Treat your mobile device like your wallet or purse

Mobile devices are valuable, not just in themselves, but because of the data they hold. Treat your mobile devices just like you would your purse/wallet or credit card. Keep them either on your person, or when not using them, lock them away. Don't leave them lying around and don't let someone else use your mobile phone unless you trust them.

Remember, if your password is saved on a device, all someone needs to do is log-in as you to gain access to any confidential data to which you have access. **It is forbidden for any member of staff to have their school emails coming directly to their mobile device without using a password log-in to access them.**

Set a password or pin number to access your device

A well-chosen password or pin number is a deterrent against casual use and abuse. A strong password should be 8 characters long and contain a combination of capitals, lowercase, numbers and symbols. It isn't complete protection as someone possessing the device can normally gain access to the contents with a bit of time and determination. However, it is a useful layer of security which will stop a casual attacker.

Don't transfer confidential data to your device

Mobile devices are small, portable and very easy to use, even when you take precautions against the event. Losing the device is a problem but losing the data on it can be catastrophic.

Wipe each device thoroughly before disposing of it

Don't just throw out or recycle your phone, it will almost certainly contain your own personal data, such as your contacts list. Ensure that is properly wiped (seek advice from your mobile phone provider).

Turn off Bluetooth

Bluetooth is a wireless protocol for exchanging data between devices. It is useful, but can also be a security risk, letting other people nearby access your phone. Only enable Bluetooth when you actually need it and then disable it again afterwards. It is a sensible precaution and will also extend your battery life.

Install available updates and anti-virus software if available

Manufacturers release updates to fix security problems and add new features. Always install updates when they are available as it is important that you get the security fixes.