Encrypting phones

1 Why?

If your data is encrypted then it cannot be read by anybody who hacks a device who does not have the password, or equivalent (you may use a finger print for instance to access your phone.)

Increasingly we expect to get our data on our phone, and this is especially true as we roll out products such as Microsoft 365. It is good news, since you can respond from anywhere without the complexity of managing a virtual private network (VPN) access. It may seem strange to an older generation, but the young take it for granted.

2 What to do

Clearly this personal data has to be appropriately secured to meet the requirements of the Data Protection Act 2018, especially as it almost certainly will be on a phone that is used personally as well as for business. (We do understand that some schools issue phones for business use only, but frequently hear that this is a nightmare to manage. We suggest that personal phones can be used, providing the owner accepts the security liability that goes with it.)

a) Passcode

The first essential is to secure the phone with a passcode, or equivalent, meaning that you have to enter data that is known only to you to "open" the phone. This does inflict an immediate restraint on personal users who might allow a child to play Minecraft to keep them quiet! Sorry, they may have to get "their own phone"; you must keep the passcode very secure.

b) Encrypt the data

Where selectable choose the option to encrypt your data (instructions below)

c) Enable remote delete

If the phone is lost, or falls into the wrong hands, you must be able to "wipe" it remotely, and once again the instructions to do that will be found below. There is a practical conflict when using a personal phone to receive business data, because your personal history will also be lost, so you must ensure that you have appropriate backup for anything that is critical to you.

3 Apple I-Phones

Essentially there are only two "operating systems" for mobile phones that we can take account of, being the Apple software and the Android operating system produced by Google. The Apple phone is very easy, personal data is encrypted by default whenever the phone is locked with a passcode or Touch ID. ... In iPhones running versions older than iOS 8, the Passcode option is under the General menu in the Settings application.

If you want to change it, go into Settings > Touch ID & Passcode > Change Passcode to update it. If you want to see if your device is encrypted, go into Touch ID & Passcode and scroll all the way to the bottom. Down there, it should say 'Data protection is enabled'.

To set up remote delete, first you must enable "find my phone", and it is best if we refer you to the proper instruction website to do this, find it here https://support.apple.com/en-gb/HT205362

Then once again to delete data we will refer you to the formal site, not least because that explains all the implications and consequences of the action that you should understand, for instance you can no longer use the location function or play a sound on the phone after erasure. https://support.apple.com/en-gb/guide/icloud/mmfc0ef36f/icloud

4 Android

This phone is somewhat more complex and you are warned that it takes time, so the phone must be well charged (or plugged in) whilst it executes, and you have to set aside an hour when you do not need to use your phone! A challenge for many!!

Before you read too much further, ensure that your phone is not encrypted by default. Google phones advise as follows:

All Pixel phones are encrypted by default. So are Nexus 5X, Nexus 6P, Nexus 6 and Nexus 9 devices. You can choose to encrypt Nexus 4, Nexus 5, Nexus 7 and Nexus 10 devices.

We recommend that in the first instance you get an overview of the two types of encryption supported, and how that applies to different releases of Android. Ideally you will have the latest release or at least 10.0 or higher, since that only supports file based encryption, all explained here https://source.android.com/security/encryption

Bearing in mind that Android is "open source" software then you are liable to get a number of sites able to provide advice, but also different "flavours" of the code. The

idea is essentially the same as Apple, in that you control the access to encrypted data with a passcode, but there are variations; please check them out here https://www.androidauthority.com/how-to-encrypt-android-device-326700/

It does define the sort of restraints that would make most people wonder if they want to do it, but it is essential in a GDPR sense. Of course if your phone choice is encrypted by default then all these questions have been answered for you, perhaps a question to ask when you next upgrade?

Similarly the find my phone feature and related remote delete need more understanding and managing with Android. Essentially you need a Google account as explained here https://support.google.com/accounts/answer/6160491?hl=en

The problem is that Google set up some restrictions to avoid accidental data loss, but you might cynically wonder whether giving them absolute control was an entirely altruistic answer!

5 Other phones

There used to be a third operating system provided by Microsoft and many Nokia phones were shipped with that installed. It does support encryption but because it is no longer maintained by Microsoft the problem becomes whether or not it is going to keep up with the ability to manage your data as Microsoft 365 or Google Docs provide future releases. We do expect further competition to emerge, and notably Huawei have announced their new system called HarmonyOS, their response to being told they could not use US technology, but it has not been shipped yet – though the Android driven P10 is encrypted by default.

6 Summary

In the future expect this to become an academic subject as all phones will be encrypted by default and have a feature to find a lost phone and be capable of deleting data remotely. If changing your phone, make it an important question to ask. As smart phones become more and more indistinguishable from computers, with data synchronisation as standard, and strong built in security, then they may become our default access – in turn requiring less paper files. Heraclitus, a Greek philosopher, has been quoted as saying “change is the only constant in life.” Died 480 BC and still relevant!!

