Knypersley First School – own devices used to process data held by the school policy

Permitting individuals to use their own devices to process personal data held by the school gives rise to a number of questions the school must answer in order to continue to comply with its data protection obligations. It is important to remember that the school must remain in control of the personal data for which they are responsible, regardless of the ownership of the device used to carry out the processing.

The underlying feature is that the user owns, maintains and supports the device. This means that the school will have significantly less control over the device than it would have over a school owned and provided device. The security of the data is therefore a primary concern. In such cases, the school will need to assess:

- what type of data is held
- where data may be stored
- how it is transferred
- potential for data leakage
- blurring of personal and business use
- the device's security capacities
- what to do if the person who owns the device leaves their employment; and
- how to deal with the loss, theft, failure and support of a device

Individuals who use their own devices to process data held by the school must take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. This includes:

- Use a strong password to secure the device used
- Use encryption to store data on the device securely
- Ensure that access to the device is locked or data automatically deleted if an incorrect password is input too many times
- Ensure that the device automatically locks if inactive for a period of time
- Make sure users know exactly which data might be automatically or remotely deleted and under which circumstances; and
- Maintain a clear separation between the personal data processed on behalf of the data controller and that processed for the device owner's own purposes, for example, by using different apps for business and personal use

How is the data transferred?
The use of own devices to process data held by the school generally involves the transfer of data between the personal device and the school's corporate system. The transfer process can present risks, particularly where it involves a large volume of sensitive information. The employee must:

- Transfer personal data via an encrypted channel
- Use public cloud-based sharing and public backup services, which you have not fully assessed, with extreme caution, if at all; and
- Take care that monitoring technology remains proportionate and not excessive, especially during periods of personal use

How will the school control the device?
The loss or theft of the device is a major risk factor given the relatively weak control that the school has on the device. The school and employee must agree how the personal data will be managed and secured. This includes:

- Register devices with a remote locate and wipe facility to maintain confidentiality of the data in the event of a loss or theft
- Make sure a process is in place for quickly and effectively revoking access to the device
- Limit the choice of devices used to those which the school has assessed as providing an appropriate level of security for the personal data being processed
- Theft or loss of the device is to be reported immediately to the Executive Headteacher

It is crucial that as data controller the school ensures that all processing for personal data is under the school's control and remains in compliance with data protection regulations, particularly in the event of a security breach. Therefore, individuals who use their own devices to process data held by the school must have the formal approval of the Executive Headteacher and formally agree to the stipulations contained in this policy.