07 Record keeping procedures

07.11 Personal Device Usage (to be read alongside 07.08 Offsite Handling & Removal of Personal /Sensitive Administration Data from the premises and home working procedure)

Key principles

This procedure applies to employees, volunteers, trustees, who use their own mobile telephones, tablets, personal laptops and PCs to access pre-school related data, particularly confidential, sensitive or personal information in relation to employees, volunteers, children, families and other interested parties.

This procedure should be read in conjunction with Little Doves Christian Pre-School policies and procedures on:

- 07.01 Children's records and data protection
- 07.02 Confidentiality, recording and sharing information
- 06 Safeguarding children, young people & vulnerable adults policy and related procedures
- Essex County Council Information Policy Requirements for Contractors v5 2022

Allowing individuals to make use of their own device(s) for pre-school purposes may result in the need for such devices to be subject to additional controls over and above those typically in place for a consumer device. Common issues and security challenges, as outlined in this procedure, must be considered when assessing the suitability of any given device to hold specific data belonging to the pre-school.

Permission will only be provided for individuals to use their personal phones, tablets, laptops and PCs for work-related purposes, where there is a good business case and strict adherence to this procedure. Approval must be sought from the manager.

During an outbreak of serious illness of disease (such as Covid-19) and the subsequent on-going after effects, there may be the need to make changes to this procedure. Any changes made will be under the direction and authorisation of the pre-school manager who will maintain a list of who is using their device for pre-school purposes. Staff are instructed to keep the manager updated and are not to operate any devices for work purposes without this permission. Any data stored on personal devices will be deleted as soon as the information is no longer required.

General Data Protection Regulation 2018

The GDPR Act 2018 requires the pre-school to process any personal data in accordance with the six key principles (see 07.02 Confidentiality, recording and sharing information and 07.06 LD Data Protection and Privacy Notice). In summary this sets out the rules in place when collecting and using personal data, how such activities may be carried out and the safeguards that must be in place to protect the data. The pre-school also processes confidential and commercially sensitive data which must also be protected.

Sensitive personal data

Sensitive personal data is information about an individual's:

- racial or ethnic origin
- political opinions

- religious beliefs or other beliefs of a similar nature
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- physical or mental health or condition
- commission or alleged commission of any criminal offence
- proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

Employees may view sensitive personal data on a personal device only if the device has a sufficiently high level of encryption. Sensitive personal data must not be stored on personal devices in any other way.

Procedure

Before using their own device for work-related purposes, an employee, volunteer, trustee must ensure that they use a strong password to lock their device. The device must be capable of locking automatically and deleting data automatically if an incorrect password is entered after several attempts. In addition, individuals must:

- use encryption software on their devices to store personal data securely; ensure that they assess the security of any open network or Wi-Fi connection and ensure unsecured Wi-Fi networks are not used
- have an up-to-date anti-virus program installed which runs regular scans of the system for unwanted and malicious services or programmes; where possible this should also provide internet filtering to prevent harmful sites from being accessed
- not download unverified or untrusted apps that may pose a threat to the security of the information held on the device
- not, under any circumstances, use corporate personal information for any purpose other than for their work and as directed or instructed by the pre-school
- ensure that they have a system of software in place for quickly and effectively revoking access that a user might gain to a device in the event of loss or theft; if possible this software should also allow remote wiping of data from the device
- make sure that any software they use is genuinely installed under an appropriate license agreement with suitable support from the relevant manufacturer to prevent any security vulnerabilities
- report the replacement of a device used for work-related activities immediately to the manager if the data on the phone was not wiped in its entirety
- report the loss, theft or replacement of a device used for work-related activities immediately to the manager
- not use public cloud-based sharing or public back-up services to store business-related personal data without prior authorisation from the manager
- wipe any pre-school data from personal devices prior to disposal or passing the device on
- not retain personal data for longer than is necessary for the purpose for which it is being used, unless there is a requirement to retain it for longer to comply with any legal obligation; if an employee is in any doubt, they should contact the manager
- ensure that if family or friends use the affected devices, they are unable to gain access to any personal

information that is work-related by, for example, by password-protection

- ensure that if family or friends use the device, they do not install applications, or disable any protective software, contrary to the procedure above

Technical support

If individuals require any technical support with their device, they should ensure that the third party providing such support has access to any data insofar as is necessary to complete their work, and that data is not transferred to a third-party device unless there is no other way of rectifying the technical problem. If data is transferred to a third-party device, the third party must warrant, and the individual must ensure, that the information is removed permanently from such a third-party device once the problem has been rectified.

Deletion of personal data

Individuals must ensure that if they delete information, it is deleted permanently rather than left in the device's waste-management system. Overwriting software may be needed to achieve this. However, this is not always practicable because, for example, the information is stored or categorised with other information that is still live. In these circumstances, it is sufficient for the individual to put the information 'beyond use', by:

- ensuring that they do not use the personal information to make any decision that affects an individual or in a manner that affects an individual in any way
- not giving any other organisation access to the personal data in any way
- surrounding the personal data with appropriate technical and organisational security
- committing to the permanent deletion of the information if and when this becomes possible

If an employee uses removable media, for example a USB drive, to transfer personal data, they must ensure that the personal data is deleted once the transfer is complete. All removable media used to hold personal data must be encrypted unless permission for the data to be in the public domain has been explicitly given by the parent/carer.

Termination of position

If an individual leaves the pre-school, they must delete all work-related personal data on their own device prior to their last day with the pre-school.

Monitoring

As part of its ongoing obligations under the General Data Protection Regulation 2018,
the pre-school will monitor data protection compliance with this procedure. Before it undertakes any monitoring exercise, the pre-school will identify clearly the purpose behind the monitoring and the specific benefits that monitoring is likely to bring. The pre-school will ensure that individuals are clear about the purpose of any monitoring and that it is justified in terms of the pre-school's requirement to comply with its duties under the Act.

Consequences of non-compliance

If an individual is suspected of breaching this procedure, the pre-school will investigate the matter under its disciplinary procedure. If any breaches are established, this could result in disciplinary action up to and including dismissal. Individuals may also incur personal criminal liability for breaching this procedure.

July 2023