## Purpose

**This policy applies to all Leafield Pre School staff that process Leafield Pre School data on personally owned devices.**

This document sets out Leafield Pre School’s policy on the use of personally owned devices to process Leafield Pre School’s data and forms part of the Leafield Pre School’s Data Protection Documentation to comply with the General Data Protection Regulation 2018 (GDPR).

Whilst it is recognised that staff use of personally owned devices for work purposes brings many benefits to Leafield Pre School such devices can pose a security risk if they are left vulnerable to theft, loss and unauthorised access whilst remote working/working from home.

This policy aims to ensure that Leafield Pre School data, which may be data about Leafield Pre School’s children’s progress and work including information that is confidential (including but not limited to information that is subject to contractual obligations to maintain confidentiality), is properly protected.

## Definitions

**Processing data** Means obtaining, recording, holding, sharing, and retaining and

deleting of Leafield Pre School data.

**UYOD** Using Your Own Device – the use of personally owned devices to undertake Leafield Pre School work or to process Leafield Pre School Data.

**Personally owned devices** Includes, but is not limited to: laptops, personal computers,

tablets and smartphones that are used to collect, store, access, transmit, carry, use or hold any Leafield Pre School data. It applies both during and outside of normal working hours and whether or not the device is used at your normal place of work e.g. at home.

**Staff** Employees (including temporary or short term workers) of Leafield Pre School.

Those undertaking placements or work experience.

Contractors engaged by Leafield Pre School

Any other individual who is working on behalf of Leafield Pre School if they are processing Leafield Pre School data or information.

**Leafield Pre School staff responsible for**

Complying with this policy.

Ensuring that their use of personally owned devices is in line with Leafield Pre School requirements to ensure data security and the protection of Leafield Pre School owned confidential information (e.g. children’s progress reports).

Ensuring that no unauthorised persons are able to access Leafield Pre School owned data (e.g. children’s names on reports) on their personally owned devices.

Ensuring that Leafield Pre School data is removed from the device before disposing of the device or selling it or passing onto another individual.

## Consequences of Non Compliance

## Leafield Pre School is bound by the GDPR, The fifth and sixth principles state:

Storage: ‘kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’);

Security: ‘processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).”

Loss of devices holding Leafield Pre School data may cause damage and distress to those who entrust us to look after their data, damage Leafield Pre School reputation and have significant legal and financial consequences. The Information Commissioner can impose serious monetary penalties on Leafield Pre School for breaches of the DPA.

Failure to comply with this policy may result in disciplinary action being taken against members of staff up to and including dismissal. In the case of breach of this policy by staff, it may lead to the termination of the engagement. This will apply whether the breach occurs during or outside normal working hours and whether or not use of the device takes place at your normal place of work. You are required to co-operate with any investigation into a suspected breach, which may include providing us with access to the device.

## Requirements

* Control access to the device (use fingerprint scanning if available, otherwise by password or PIN if neither fingerprint nor password is possible).
* Use a screen or device lock that will trigger after a short period of inactivity (no longer than 10 minutes).
* Keep your device’s software up to date. This includes operating systems, applications, and anti-virus and malware protections.
* On leaving Leafield Pre School, ensure all Leafield Pre School data is deleted securely from your device. Ensure that master copies of documents that are required by the Leafield Pre School are transferred to other Leafield Pre School staff before you leave.
* Remove Leafield Pre School data from the device before disposing of the device or selling it or passing onto another individual. Ideally, the device should be reset to factory defaults.
* Do not leave your device unattended in situations where others could access it. Do not share your device with others, including members of your household.
* The loss or theft of a personal device that holds any Leafield Pre School data or where you believe that the device may have been accessed by an unauthorised person or otherwise compromised, must be reported as soon as possible to Leafield Pre School Manager.

## Key Points

All staff must comply with these key points:

* The contents of our systems and Leafield Pre School data remain Leafield Pre School property. All materials, data, communications and information, including but not limited to, e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device during the course of your work for Leafield Pre School or on its behalf is the property of Leafield Pre School, regardless of who owns the device.
* Leafield Pre School data held on personal devices is subject to Subject Access Rights under GDPR and must be provided to Leafield Pre School office on request.
* Avoid processing personal data on personally owned devices whenever possible.
* Some devices may offer an automated backup facility which stores a backup of data on the device to the user’s cloud-based account or to the user’s personal computer. Leafield Pre School require that no Leafield Pre School Data is saved to a personal Cloud account.
* You must pay for your own device costs under this policy, including but not limited to voice and data usage charges and any purchase and repair costs. By using your device for Leafield Pre School related purposes and unless otherwise agreed with you in a separate agreement with the Leafield Pre School you acknowledge that you alone are responsible for all costs associated with the device.
* Consider security of third-party software (apps) i.e. untrusted and unverified market-places. Such untrusted sources may have a higher prevalence of malicious apps. You must also take care not to overstate the guarantees that an ‘official’ market-place may offer. Such outlets may only provide cursory glances at applications and fail to block all instances of malware.
* Usage of UYOD could raise the risk that personal data is processed for a purpose different from that for which it was originally collected. You must ensure that users of devices know their responsibilities in terms of only using corporate personal data for corporate purposes.

All staff and others who work on behalf of the Pre School must report any loss or suspected loss, or any unauthorised disclosure or suspected unauthorised disclosure, of any Pre School owned data immediately to office@leafieldpreschool.org.uk in order that appropriate steps may be taken quickly to protect Pre School data. Failure to do so immediately may seriously compromise Pre School data and, for staff, may lead to investigation and potentially action under the disciplinary procedures.