Remote and Homeworking Policy

Version	Purpose/Change	Author	Date
1.0	Initial version	Will Harries	01/02/2019
1.0	Reviewed	Will Harries	03/02/2021
1.1	Reviewed	Jessie Kazak	15.3.24

To be reviewed: 15.3.26

Definitions

The Kindergarten	Laurel Farm Kindergarten, a registered charity.
Staff	Any person undertaking work directly relating to the Kindergarten, whether paid or otherwise. This includes the Board of Trustees.
Remote working	The undertaking of work directly relating to the Kindergarten, away from the Kindergarten grounds.
Sensitive data	Any information directly related to the work of the Kindergarten. This includes but is not limited to personal information of staff, members and children, learning journals, invoices.

Summary

The Kindergarten will, where appropriate, provide staff the equipment and opportunity to work from locations which are remote from the Kindergarten site. All staff who work remotely must ensure that they are aware of the acceptable use and storage of both IT equipment and printed documents.

The purpose of this document is to state the remote and homeworking policy of the Kindergarten.

Equipment, whether IT or otherwise, is provided to staff to enable them to conduct the Kindergarten's business efficiently and effectively. The equipment, any information stored on it, and any printed Kindergarten documents should be regarded as valuable and sensitive information should be safeguarded appropriately.

This document applies to all staff of the Kindergarten.

This policy should be adhered to at all times where a member of staff is working away from the Kindergarten site.

Risks

The Kindergarten recognises that there are risks associated with staff accessing and handling information in order to conduct the Kindergarten's business.

The mobility, technology and information which makes portable IT equipment so useful to users also make them valuable to thieves. Securing Kindergarten information, both electronic and physical, is an incredibly important issue.

This policy aims to mitigate the following risks:

- Unauthorised access to protected and sensitive information
- Equipment damage, loss or theft
- Accidental or deliberate overlooking by unauthorised people

- Introduction of malicious software and viruses
- Sanctions against Laurel Farm Kindergarten by the ICO as a result of a data breach
- Legal action against the Kindergarten as a result of a data breach

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in financial loss and an inability to provide services to our members.

Benefits to Staff

- Promotion of work/life balance
- Job satisfaction
- Flexibility
- Saving of travel costs and time
- Reduced stress

Benefits to the Kindergarten

- Staff attraction, retention and performance
- Promotion of the Kindergarten as forward-thinking and able to embrace technology, maintaining operational flexibility

Applying the Policy

- All equipment supplied to users remains the property of the Kindergarten unless expressly stated
- Equipment must be returned at the request of the Kindergarten
- All IT equipment will be supplied and programmed by the Kindergarten
- Software must only be provided by the Kindergarten

Staff Responsibility

- Staff must take due care and attention of equipment when moving between office, home and any remote location
- Staff will not install or update software to any IT equipment unless expressly agreed by the trustees
- Users will not change the configuration of any IT equipment unless expressly agreed by the trustees
- Users will not install any hardware to or inside any IT equipment
- All equipment faults must be reported to the staff member’s line manager

- User registration on IT equipment must be requested from the trustees
- IT equipment must not be used for personal use by staff
- Staff must ensure that reasonable care is taken of equipment. In transit, equipment will be stored out of sight in the locked boot of the vehicle if it is necessary to leave unattended
- Permission to work remotely must be sought from the staff member's line manager
- No equipment must be kept away from the Kindergarten grounds any longer than necessary. If it is required that equipment be kept away from the grounds for longer than a week, this must be agreed by the staff member's line manager and the trustees must be notified.
- The remote working environment must be one in which the staff member can concentrate without unnecessary distraction.

Remote Working Arrangements

Staff should be aware of the physical security dangers and risks associated with working within any remote working location, including at home.

Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. Equipment must be secured whenever it is not in use. If left in an unattended vehicle, equipment will be locked in the boot out of sight.

Staff must ensure that usernames are kept in a separate location to the portable computer device at all times. Passwords must, as far as practically possible, not be written down. If they must be stored physically, they must be stored securely and in a separate location to both the portable computer device and the username.

Paper documents are vulnerable to theft: these should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use. Sensitive documents should be collected from printers as soon as they are produced and not left where they can be casually read. Waste paper containing sensitive information must be shredded.

Staff shall ensure that appropriate security measures are taken to stop unauthorised access to sensitive information, either on IT equipment or in printed format. If unauthorised access occurs, the trustees must be notified immediately.

Access Controls

It is essential that access to all sensitive information is controlled. This can be done through physical controls, such as ensuring that documents and removable media devices are held securely or by locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password protection or user access controls.

IT equipment should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes. All data on IT equipment must, where possible, be encrypted. If this is not possible, then all sensitive data held on the device must be password protected.

Anti-Virus Protection

Ant-virus software will be installed on all portable computer devices before being given to staff. Staff must allow the scheduled updates of the anti-virus software.