The Learning Partnership
Bedfordshire & Luton Ltd
Making a difference to learning in the communities

Policy
Lone & Remote Working

Introduction

The Health and Safety Executive define lone workers as those who work by themselves without close or direct supervision. This includes staff in offices where only one person works – or is working – and staff working alone away from the office.

Remote working is a variant of lone working where individual staff are employed on outreach or are embedded in other organisations, including stakeholders and partners. Remote working is also a factor from time to time for office based staff.

Lone Working in the Office

There may be occasions when an employee is working alone in the office with no-one else in the vicinity or rest of the building. In these circumstances:

- the outside door to the central column stairway should always be locked
- no member of the public / partnership agencies is given admittance to the building (without prior knowledge of the purpose of their visit).
- any feeling of insecurity should result in an immediate vacation of the building, (including the securing of the premises, if possible), followed by a call for help to another employee or the emergency services

An employee may decide to work immediately before or after the working day in order to fulfil a particular task. The employee's line manager must agree to this.

Any unusual event, phone call or concern experienced by an employee should be recorded in the incident book and subsequently brought to the attention of a person's line manager.

No employee should host or facilitate an out of hours meeting alone but should arrange for another employee to be there at the same time and in the same place

Away from the Office

When staff members are working away from the office, they must:

- inform their line manager of their meeting schedule by means of recording their plans on the outlook diary. This should include the location, start and finish time, contact telephone number and the time expected of the next appointment or back in the office
- confirm the arrangements for the start of the normal working day / finish of working day as appropriate on the outlook diary

Arrangements for working away from the office outside normal hours must be noted formally by an employee's line manager.

Members of staff should not normally arrange to work away from the office with clients on a 1:1 basis outside normal working hours and outside public buildings. An employee must seek approval from their line manager for such work.

Any unusual event or concern should be noted in the incident book and subsequently brought to the attention of an employee's line manager.

Arrangements for Remote Workers

Employees who are remote workers understand that by using their personal computer equipment that they are responsible for any loss, damage or wear to the personal computer equipment.

Employees are also responsible for taking precautions so that only authorised individuals can gain access to any confidential or restricted information that is stored or accessed from their computer. This includes securing any private wireless home network by using encryption or security settings.

Employee Responsibilities - Computer Equipment

Wherever possible employees should ensure the equipment used to remotely connect to Partnership servers is up to date with all known operating system updates and patches.

Automatic Updates should be switched on if Microsoft Windows is installed. The User should ensure the equipment used contains an anti-virus program which is updated on a regular basis (preferably automatically). It is also a condition that the employee uses a personal firewall programme supplied with the equipment.

The company cannot provide technical support for personal computer equipment including PCs, laptops, printers, routers and / or internet connections.

Confidentiality and Access to Data

Employees must take all necessary precautions so that unauthorised individuals cannot view confidential information that appears on the screen when accessing the Learning Partnership network or any other relevant database in line with normal business and the employee knows and understands his/her obligations under the Data Protection Act 1998.

The employee understands that no Partnership data or information may be copied, reproduced, distributed, downloaded, posted or transmitted externally without the prior written permission of the company.

Any breach of this will be vigorously pursued in accordance with the Computer Misuse Act 1990.

Employees must not share their passwords, SMS Codes or security fob with anyone else unless authorised to do so by their line manager. Lost or stolen fobs should be immediately reported to their line manager.

Disposal of Confidential Information

Employees are responsible for the proper disposal of confidential information if removed from the office to enable remote working. Any printed documents containing confidential information must be returned to the office for proper disposal in a shredder bin or shredded by the user using his or her own personal shredder.

The employee agrees to abide by software licensing, IT acceptable usage policy set down in the IT Policy or other applicable document and any security agreements communicated to them at any time.

The employee understands that his/her actions, activities and printing may be audited, monitored and/or recorded whilst he/she is working remotely.

Ownership of Data

Employees do not have any rights or ownership interests in any confidential or restricted information belonging to the company and must appropriately dispose of any information of this type that may be stored on their personal computer or in printed form once they are no longer employed by the company.

Upon leaving or ceasing to work for the company all equipment issued will be returned by the employee to their line manager. Failure to do so will result in a deduction from their final salary payment or invoice to cover cost of replacement and administration costs.

Lost, stolen or damaged equipment will be replaced at a charge per device. Such charges shall be recovered through a payroll deduction, except in exceptional circumstances when agreed by the Management Team.

Risk Assessment

Health and safety is the responsibility of the employee in relation to the use of personal computer equipment and remote or lone working. In this case the company health and safety officer will conduct an annual risk assessment and discuss the results with the individual concerned.

Approval

Signature:			S Kendall - Chair
Board Approved:	October 2015	Review Date:	July 2016