LONE & REMOTE WORKING POLICY

Purpose of Lone & Remote Working Policy

This policy aims to ensure Beacon East staff/associates working on behalf of Beacon East have full knowledge of the expectations and appropriate work behaviour when working alone or remotely. It also aims to ensure the person is aware of any possible hazards and risks to which he/she may be exposed to. The person will know what to do if something goes wrong when working remotely. Beacon East and the partner school(s) are aware of the whereabouts of the lone worker. They are also fully aware what work he/she is engaged in and on what date this work is taking place. There are agreed and appropriate systems/procedures in place with partner school(s) to ensure, not only health & safety, but also safeguarding and data protection are fully adhered to in line with the latest government legislation. Beacon East staff/associates will also be made fully aware of the partner school(s) policies on remote working, safeguarding and data protection before supporting any students at their school(s).

It is recognised that many Beacon East staff/associates, by the nature of their work, can be required to work alone or remotely. Lone working can be described as “work that is specifically intended to be carried out by unaccompanied persons, without direct supervision or immediate access to another person for assistance”. Lone working may expose employees/associates to additional health & safety risks, which do not present themselves in other circumstances. It may also expose that person and the recipient(s) of the work to possible safeguarding and data protection issues. Through a process of risk assessment, significant risks will be identified and controls put in place to eliminate/reduce the risk. To achieve this, the co-operation of all involved, including the partner school(s) is essential and requires all levels of management and individual staff members/associates to work together to develop and implement local safe systems of work. To this end, this document has been developed in support of the Beacon East member of staff/associate and those who they work with. This policy aims to ensure the lone worker has full knowledge of the possible hazards and risks to which he/she is being exposed.

Remote working may be required from time-to-time and it may be appropriate in order to keep a valuable service for young people going e.g. careers advice. This remote service may take place from a Beacon East member of staff or associate’s home. This can only take place if this person fully adheres to Beacon East and partner school(s) policies/guidelines on remote working, safeguarding and data protection. That person should also operate in line with government legislation. There should be agreed and appropriate systems and virtual platform(s) in place before any remote work takes place. Remote work can only happen if it has been fully agreed by the partner school(s), Beacon East management and the Beacon member of staff/associate. Beacon East is committed to ensuring, so far as is reasonably practicable, that staff/associates who are required to work alone or unsupervised for significant periods of time are protected from risks to their health & safety. Working alone does not contravene the law, but it can bring additional possible risks to a work activity. Through the process of risk assessment

staff/associates will identify activities that have any significant level of risk attached to them or recipients of the work they deliver. Beacon East will, so far as is reasonably practicable, employ controls and work in partnership with schools to reduce the exposure to those risks or eliminate the risk all together.

Scope of policy

This policy applies to all Beacon East employees/associates undertaking work on behalf of the company and refers to all services and activities of Beacon East. It is applicable to all lone workers, advisers, associates and staff who are not routinely defined as lone workers but on occasion are required to work alone or remotely as per the definition. This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on: Teaching online safety in schools · Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff · Relationships and sex education · Searching, screening and confiscation It also refers to the DfE's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a good reason to do so. It is very important that Beacon East staff/associates fully understand the importance of the above and fully understand the responsibly they have when providing support for young people remotely.

Responsibilities

The CEO (Mark Bruhin) is responsible for ensuring that staff/associates are aware of this policy and they understand the methods and timing of reporting any incidents. Ensuring risk assessments, local policies and procedures are produced and that safe systems of work are adopted including emergency response arrangements. Ensuring that any lone/remote working procedures and safe systems of work implemented are subject to regular monitoring and reviewing to ensure effectiveness. All Beacon East staff and associates have the responsibility to fully understand Beacon East polices, partner school(s) policies and government legislation on lone/remote working. They also have the responsibility to raise any concerns and report any incidents to the appropriate persons at Beacon East and partner school(s) immediately. It is understood that the partner school(s) also have a responsibility to ensure safe working procedures and systems are in place before any work commences. The partner school must provide evidence of their policies on remote working, cyber security, safeguarding and data protection. Beacon East and staff/associates must be fully satisfied this is all in line with the latest legalisation before any partnership work commences.

Beacon East staff / associates must:

- Before any work commences, ensure they have all the necessary policy information, instructions and training to recognise the hazards and risks involved with working alone or remotely on behalf of Beacon East.

- Comply with policy and related procedures and co-operate with managers and partner school(s) on all health & safety, safeguarding, cyber security and data protection matters.
- Attend any appropriate training.
- Take reasonable care of their own health & safety and that of others who may be affected by their work.
- Advise Beacon East and partner school(s) of any concerns or risks they have identified before any remote work commences.
- Follow safe working procedures as agreed with Beacon East and partner school(s), including the use of IT and cyber security when working remotely.
- Share their work schedules with Beacon East and partner school(s) before remote work commences.
- Ensure they are fully contactable by Beacon East management and partner school(s) during those contracted hours.
- Report any incidents immediately to the appropriate persons at Beacon East and partner school(s).
- Co-operate fully in any subsequent investigation of a reported incident.

Monitoring and Review

Beacon East is committed to ensuring that all policies and procedures are kept under review to ensure that they remain compliant with all relevant legislation and reflect organisational development. This policy document will be reviewed by the CEO and company management by the date indicated on the document footer, or earlier if required. Beacon East is committed to regular auditing of lone/remote working arrangements and will also monitor agreed performance indicators.

Remote Working

Definition: Remote working is a work arrangement that permits an employee or associate working on behalf of Beacon East to conduct all or some of their work at an approved alternative worksite such as their home. This policy has been developed to protect sensitive or valuable data and maintain the overall security whilst Beacon East associates/employees are working remotely. In addition, this policy recognises and defines the duty of care of both Beacon East and the partner school(s) in regard to the remote worker and their health & safety and fair treatment. Beacon East associates/employees must ensure security of information and systems accessed through mobile and remote working arrangements are given due consideration. This policy emphasises the importance of staff understanding current information security policies and procedures and each individual's responsibilities in relation to these which must be adhered to at all times. Information that is related to and can identify an individual is called personal data and is protected by the principles of the Data Protection Act 1998 and the following GDPR Act 2018.

Eligibility and Process

In principle, any job role at Beacon East could be considered for remote working. Nevertheless, it is clearly the case that some activities can only be adequately carried out on-site, whilst others may be carried out equally or even more effectively at a remote location, usually the employee's home. A proposal to conduct remote working needs to be carefully reviewed in terms of: the use of equipment; health & safety and communications considerations; security, data protection, and other legal issues; working and reporting relationships and any requirements to attend work to perform the duties of the post. For a role to be considered for ad hoc remote working, the employee must submit a request with reasonable notice to their line manager who will consider the effectiveness of the role being performed off site and the impact on any direct reports. For a role to be considered for regular remote working, the employee must submit a flexible working request to their line manager who will consider the request under the company's flexible working policy. The Remote Working Policy should not be used as an alternative to caring for dependants.

Security

Personal Security

For the maintenance of personal security, Beacon East strongly advises against any external work contacts visiting an employee/associate when they are working at home and that such physical visits should take place on the school premises wherever possible. For the employee's/associate's own security it is also recommended that employees who are remote working should:

• Not release any personal data or information to external contacts such as home address or personal e mail address and telephone number.

• All employee/associate remote working business lines should be ex-directory or unknown.

• Always ensure that Beacon East and partner school(s) are fully aware of the remote working and that person's whereabouts and that they can be easily contacted within the agreed contractual working hours.

Security of client data and IT when working remotely

- To ensure safety and security is maintained at all times, an appropriate room should be allocated for remote working.
- The IT equipment used for remote work should be appropriate and checked.
- The IT equipment used should have a range of security measures enabled to make home working safer. Keeping the device password-protected (strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters).
- Minimise any storage of client data at home.
- When accessing client date via school database it must only accessed with the permission and guidance of the partner school(s). It must be locked before and after access has taken place. Access must be in line with the school policy who have allowed access to their client data base. Data should not be removed from the database or shared elsewhere.

- Beacon East safeguarding and data protection polices must should be adhered to when remote working; this includes locking a device when not in use, ensuring that data is encrypted in the event of device loss and not disclosing any passwords, PINs or encryption keys. It is the responsibility of the remote worker to safeguard and protect any information that they hold.
- Remote workers must have an understanding of digital risks, use secure working practices and apply encryption and back-up procedures as appropriate. If the remote worker is not confident in this area, they should seek assistance from IT User Support team prior to working remotely.
- Digital information must only be downloaded or uploaded over a secure connection. For example the types of WiFi networks offered to travellers at airports, hotels, coffee shops and on public transport are generally insecure and therefore must not be used for remote learning. Unsecure network compromise data and internet security and therefore the safe guarding of young people.
- The remote worker must only use an appropriate and reputable virtual platforms to conduct their remote work e.g. MS Teams, Google Meet or Zoom. It may vary from school to school. It is important that the platform is fully agreed by both parties and the remote worker is fully comfortable when using the platform not only terms ensuring quality of delivery but ensuring security. If training or support is required this must raised with Beacon East as an issue to be resolved.
- Invitation from the agreed virtual platform should allow the student to join the meeting. If they do not join the meeting, please ensure there is an agreed system in place with the partner school(s) to alert the line managers of the failure of a student to attend a virtual meeting or activity.
- Any calls made from home/mobile must anonymous e.g. by putting 141 on the beginning of your mobile phone number. You must not give out the phone number and only e mail students by using the work/school careers e mail address.
- During interview you are encouraged to se the camera image so it has a blurred background so that students cannot see into the staff/associate home.
- When sharing pages e.g. careers web sites or documents you must ensure they appropriate to the work agreed with the partner school(s).

Health and Safety

The underlying principle of this section is that the standards of care towards remote working should be equivalent to that of employees/associates working on the school premises. Therefore, it is essential that work from an staff/associate's home or elsewhere does not adversely affect the health & safety of the remote worker or others. It is the duty of the Beacon East employee/associate to ensure the equipment and working practices meet the standards as defined work with display screen equipment: Health and Safety (Display Screen Equipment) Regulations 1992 as amended by the Health and Safety (Miscellaneous Amendments) Regulations 2002. To ensure this is met, the employee/associate must conduct a Display Screen Equipment risk assessment within the first week of remote working. While the Beacon East has a reasonable duty of care towards an employee's/associate's health & safety, the employee/associate undertaking remote working, is expected to take primary responsibility for ensuring safe and healthy working conditions whilst working offsite. Therefore, prior to commencing remote working on regular basis, a DSE Health & Safety Risk Assessment should

be completed Employees are encouraged to seek further advice and guidance on how to set up a remote working workstation. It is the joint responsibility of the manager and employee/associate to ensure that a thorough risk assessment is completed prior to starting regular remote working. In addition, a review of the risk assessment should be conducted on an annual basis as a minimum. If in the event, further clarification or advice is needed, the manager and employee/associate should ensure they consult with the current Health & Safety guidelines. Beacon East and the partner school(s) have the right to refuse to allow remote working on grounds of health & safety.

Work terms and conditions

Remote working employees/associates maintain their existing terms and conditions of contract employment apart from their designated place of work, which changes from the school to the remote worker's defined remote site. Prior to commencing remote working the employee/associate should agree on the working pattern and the times they will be available for contact. If either party request the remote working arrangements to end, a reasonable period of notice should be given and agreed to allow both parties time to consider and plan alternative arrangements. To ensure the remote working arrangement is effective, reviews will be conducted by the line manager to ensure the business needs are met and the arrangement is still efficient. Remote working agreements will be reviewed at least quarterly to ensure the arrangement continues to meet any change in business demands. Remote working agreements may also be reviewed as a result of any team or company organisational changes.

Lone Working

Sources of Advice and Further Information

Further advice and information regarding lone working can be obtained from the Health & Safety Executive. This document should be read in conjunction with related policies and procedures e.g. Health and Safety at Work Policy Risk Management Strategy, Equality and Human Rights Considerations. This document has been screened for equality implications as required by Section 75 and Schedule 9 of the Northern Ireland Act 1998. Using the Equality Commissions screening criteria, no significant equality implications have been identified. It is therefore not subject to equality impact assessment. This document has been considered under the terms of the Human Rights Act 1998 and was deemed compatible with the European Convention Rights contained in the Act Records Management. The supply of information under the Freedom of Information does not give the recipient or organisation that receives it the automatic right to re-use it in any way that would infringe copyright. This includes, for example, making multiple copies, publishing and issuing copies to the public. Permission to re-use the information must be obtained in advance from Beacon East.

LONE WORKING PROCEDURE

Risk Assessment and Safe Systems of Work

Risk Assessment includes:

STEP 1	**Identification of individual, environmental and service provision risk factors.**
STEP 2	**Development of local procedures to implement the outcome of the risk assessment.**
STEP 3	**Providing information to all staff that are affected.**
STEP 4	**Regular reviews are necessary at regular intervals and whenever there is reason to suspect they are no longer valid.**

STEP 1 - IDENTIFICATION OF RISK FACTORS

The risk assessment process should take into account the identification of hazards from; for example, means of access, equipment, substances, environment, travel/route planning, communication, activity, individuals etc.

Particular consideration should be given to: -

Individual Risk Factors

Client/Other Individual: Is the person facing high levels of stress, likely to be drunk or on drugs? Does the person have a history of violence? Does the person have a history of criminal convictions? Does the person suffer from a medical condition, which may result in a loss of self-control?

Staff/Associates: Are staff/associates familiar with relevant Beacon East policies and local arrangements for lone workers and have they received relevant training? Are the staff new to the job, location or caseload? What is the staff medical fitness? Special needs or disabilities of a member of staff may have to be taken account of. This is applicable under general health & safety legislation and the Disability Discrimination Act. Working with Groups: Is the history of the group/area a factor? Have you a planned exit route? Are there people attending from other services/agencies?

Environmental Risk Factors: Is the remoteness or isolation of the workplace a factor? Are there any problems with communication? Is there a possibility of interference, such as violence or criminal activity from other persons? Is there a possibility of an animal attack? Position within the room? Are there offensive weapons present?

Service Provision Risk Factors: Has the person verbally abused a member of staff in the past? Has the person threatened an adviser with violence in the past? Has the person attacked or attempted to attack an adviser in the past? Is the work out of hours? Does the person have unrealistic expectations of what can be done for them? Does the person perceive staff as wilfully unhelpful?

STEP 2 - DEVELOPMENT OF LOCAL PROCEDURES / SAFE SYSTEMS OF WORK

From the risk assessment it should be possible to identify lone working risk areas or activities. Local procedures need to be written to ensure there is a safe system of work for staff working in lone worker risk areas or activities. The emphasis should be to reduce the risk to as low as is reasonably practicable.

STEP 3 - COMMUNICATION

The risk assessment should pay particular attention to the process of communication.

Sharing of Information between services/other agencies. There should be communication of information about patients/clients/significant others between services/other agencies, which may be providing service to the same individual. This should be documented. All relevant disciplines providing service should be informed about the risk, potential for violence and aggression, including trigger points. The management is responsible for ensuring systems are in place to share such information and concerns. Balancing the need to provide information on potential risks in protecting an individual's right to privacy.

Local system of communicating with each other.

It is imperative that the team leader or manager establishes a local system of communicating the whereabouts of individuals and an emergency response system is agreed. All staff/associates must be compelled to use the system once established. A communication procedure must be in place in every location/team and be utilised by all staff/associates.

MONITORING & REVIEW

Beacon East management will ensure that any lone working procedures and safe systems of work implemented are subject to regular monitoring and reviewing to ensure effectiveness. This may take the form of both informal monitoring on a day to-day basis and more formally via safety inspections. Risk assessments must be reviewed at regular intervals and whenever there

is reason to suspect they are no longer valid. Staff/associates are responsible for adhering to procedures and should report any incidents or concerns relating to the safety and effectiveness of the working arrangements to their line manager. It is the responsibility of the individual and the line manager to identify any training needs and to ensure that these are facilitated, for example.

REPORTING SYSTEM

Incident Management: All incidents must be reported to the CEO (Mark Bruhin) and partner school immediately.

- Share details of both your work schedules for the day and your vehicle and travel details i.e. destinations and expected times of arrival/departure.
- Let them know of any changes to your schedule even small changes.
- Confirm with base that you have returned or the visit has ended. Arrange for contact/emergency response if your return is overdue.
- Communicate via mobile-phone/telephone to highlight any visit or situation causing concern.
- Lone workers such as advisers may wish to inform someone they are working alone and contact them again to confirm they have finished work and left the premises.

When at attending school sites or events

On Arrival

BE ALERT, BE AWARE, BE SAFE

- Park with care, in such a way as to ensure a quick getaway.
- Be aware of your attitude, body language.
- Keep clear of the doorway after ringing and stand sideways on so you present a narrow, non-threatening but protected stance.
- Introduce yourself and the reason for your visit.
- Always show your Beacon East ID card.
- Do not enter if the person you are calling to visit is not available.
- Be aware of your surroundings and exits. Try to sit nearest the door.
- Remain aware of the behaviour of all persons in the area, watching for changes in mood, movements or expressions that may indicate a problem.
- Never give your home telephone number or address.

IF AT ANY TIME YOU FEEL YOUR SAFETY IS AT RISK, OR VIOLENCE IS THREATENED LEAVE IMMEDIATELY AND SEEK HELP.

ON RETURN

If something has happened during your visit which has caused you concern or has caused you to feel threatened. Inform your line manager and discuss further action.

HIGHER RISK VISITS/LOCATIONS

Visits assessed as higher risks should only be undertaken if considered essential. More stringent control measures need to be detailed in the local policy and procedure. It may be

appropriate to call the point of contact immediately before and immediately after some visits, joint visits or an escort may be necessary, use of local taxis may require consideration etc. For visits to higher risk locations (for example, areas with high-crime rates, isolated rural areas etc) an assessment of the situation and needs should be made before leaving and any additional checks that may be required should be made. If you have any doubts regarding the location: Double check the address, telephone number and consider ringing back to confirm the validity of the location.

SEVERE WEATHER CONDITIONS

If weather conditions are severe and roads are unsafe, do not put yourself at unnecessary risk. Staff must communicate with their line managers and colleagues to inform them that they are going on a visit, where, how long, what route etc. If your visit is essential, make sure you are prepared for any eventuality including a means of communication.

CAR SAFETY

By keeping your motor vehicle in good working order, reporting any faults and carrying out regular servicing you will limit the risk of breaking down. Simple pre-driving checks will also help, such things as:

- Fuel in tank extra fuel in a safety-approved can
- Oil level to correct level water in radiator Spare tyre is inflated
- Horn & lights working water in washer bottle and washers work.
- Do you know how to change a wheel, where your fuses are in the car?
- Do you have spare fuses?
- Do you have details of breakdown/rescue organisations?

IF YOUR CAR BREAKS DOWN

- Turn on your hazard warning lights, (notify base/colleague) and summon assistance as appropriate.
- Try to assess whether it is safer to stay in your car, or to get out, take account of how isolated you are and the time of day.
- If you stay inside, sit in the passenger seat to give the impression you are not alone.
- Display a “help” notice if you stay in the car.
- Keep your doors locked and the window open no more than 1.5 inches, if someone stops to offer help, ask him or her to telephone the police. Do not let people who offer to help get into your car.
- If you leave the car, lock it and note its location, if you have a personal alarm, take it and keep it in your hand. If it is dark, or will be soon, take a torch.
- If you have a warning triangle, place it in the direction of on-coming traffic, 30 metres from your car and on the same side of the road.

PERSONAL SAFETY IN YOUR CAR

- Make sure you carry your mobile phone with battery fully charged or coins/phone card for an emergency.
- Plan your route before setting off, when you have the choice use main roads.
- Tell someone the route you will be taking and when you expect to arrive.
- Let someone know if you change your journey plans.
- Have the directions and maps in the car so you do not have to stop to ask.
- Try to travel on main well-lit roads.
- Keep aware of the latest police recommendations regarding road rage. For example, if another driver gets annoyed with you. Do not make eye contact or make gestures.
- Do not have valuables visible in the car when driving.
- Stay in the car as much as you can. Keep the doors locked and windows closed, especially in towns where you will be stopping at junctions.
- Keep handbags, briefcases and mobile phones out of reach of open windows in case of snatch thieves.
- When you leave the car, lock personal belongings, equipment, drugs etc in the boot, not on display.
- Lock your car, even if you are only going to pay for petrol on a garage forecourt.
- When parking in daylight, consider what the area will be like in the dark.
- At night, park in a place, which is well lit, and if possible busy. Try to avoid car parks or areas where you and your vehicle are not clearly visible
- Have the keys ready before you get into the car, check the back seat.
- If you see an incident or accident, or someone tries to flag you down seek assistance, ask yourself if it is genuine and if you could really help – it might be best to phone for help or drive to the nearest Police station.
- If a car pulls up in front of you and you have to stop, keep the engine running. Stay calm and ensure all the doors and windows are locked. If the driver leaves the car to approach you, reverse as far as you can while sounding the horn and activating the hazard lights.

- If you think you are being followed, try to alert other drivers with your lights and horn. Phone or pretend to phone the Police and make an obvious note of the car registration number. Keep driving until you reach a busy area or a police/fire or ambulance station or even a garage.
- Never give lifts to strangers.

PERSONAL SAFETY ON FOOT

- Avoid wearing clothing or accessories that could be used to harm you e.g. scarves, ties, heavy necklaces.
- You are more likely to escape danger wearing clothes you can move in easily and shoes that are comfortable; walking quickly is usually safer than trying to run.

- Valuables, such as wallets should be kept in an inside pocket and secured, or use a body belt or “bum bag”, try to keep both hands free.
- To carry things, use a small bag slung across your body under a jacket or coat, or a shoulder bag with a short strap and secure fastenings, make sure it sits close to your body with the fastening innermost.
- Carry in your pocket coins/phone card and the telephone number to stop all your cheque cards and your keys.
- Whenever possible, avoid walking alone at night or near groups of rowdy people.
- Keep to busy, well-lit roads.
- Do not take short cuts, unless you know they are as safe as the longer route.
- Avoid poorly lit or little used underpasses, waste ground and isolated pathways especially at night.
- Carry a torch. Walk facing oncoming traffic.
- At night or in bad weather conditions where visibility is poor ensure you wear a high visibility jacket.
- Have a personal alarm readily at hand (available from Health & Safety).

Additional useful links on remote and lone working

Keeping Children Safe In Education

https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

CPNI – Remote Working

https://www.cpni.gov.uk/system/files/documents/d2/4e/REMOTE%20WORKING%20%202020-%20FINAL.pdf

HSE – Protecting Lone Workers

https://www.hse.gov.uk/pubns/indg73.htm

Local Government Association – top tips

https://local.gov.uk/our-support/workforce-and-hr-support/wellbeing/remote-working-top-tips

If there are any questions regarding this policy please contact:

Mark Bruhin (Beacon East CEO)

E Mail: mbruhin@beacon-east.co.uk

Tel: 01603 673340 / 07766 056330