DAB VJB

Dunbartonshire and Argyll & Bute
Valuation Joint Board

Guidance on Flexible (Agile) Working

Document Control

Version	Date	Author	Summary of Changes
0.1	March 2021	D Thomson	Joint Board adaptation of WDC "Workforce of the Future" Guidance on Flexible Working
0.2/0.3a/03b	April/May/June 2021	D Thomson	MTM iterations
MT approved	June 2021	D Thomson	Minimal change – approved version for Union consultation
Board approved	15 September 2021	D Thomson	None – Board approved version

1. Introduction

Dunbartonshire and Argyll & Bute Valuation Joint Board (the Joint Board) recognises the demand to create an attractive workplace with:

- modern working practices which enhance service delivery through people working in new and different ways
- the aim of achieving a better balance between home and work life demands.

'Agile Working' is about ensuring the Joint Board supports a flexible and skilled workforce by introducing more flexibility around how and where employees carry out their work, enabling them to maximise their productivity and performance. Flexible work styles enable employees to work from home as agreed with Line Managers.

2. Aim of the Guidance

Managing employees and teams with differing work styles and working arrangements presents a unique set of challenges and opportunities. This guidance sets out the key elements of managing and supporting a flexible approach to work. The aim of the guidance is to ensure fair and consistent processes are followed and both managers and employees know what is expected of them when working in such a way.

3. Scope

Ways of working such as flexible and home working, are commonly referred to as 'agile working'. This is the term used throughout this guidance to describe new ways of working which facilitate employees adopting new work styles and operating in different work settings or locations.

This guidance will apply to all Joint Board employees and supports (but does not supersede) any other flexible working and employment policies and procedures that already exist for employees. All of the Joint Board's employee terms and conditions of service, policies, procedures, and guidelines, including sickness reporting, booking of annual leave, requesting time off in an emergency, etc, are unchanged and will still apply to those working in a flexible manner.

All Joint Board posts, with the exception of the post of Caretaker, may be considered for a blend of office and home based working (with the assumption that survey and inspection can be carried out commencing from either).

4. General Principles

Agile working allows increased flexibility for both the employer and employee but also comes with responsibility to ensure that any agreed arrangements do not negatively impact on service delivery. Some general principles which must be upheld in applying this Policy include:-

- Service Provision must remain the priority for all involved. Where the service requires an office and/or public facing presence this must be maintained at all times.
- All workloads and tasks must be shared by relevant staff (though not necessarily at any one point in time)
- Training – either formal or informal – cannot be compromised. To this end, the employee and the line manager must consider the role of both trainers and trainees.
- Subject to existing contractual arrangements and work patterns, employees must be available to attend the workplace, including for meetings, one-to-ones with managers and for any other purposes as required by the line manager. This requirement extends to any requirement, for example, to make ICT hardware available for installations and upgrades.
- All staff must be contactable during agreed working hours.
- The option to work from home from time to time is available to employees on a voluntary basis. No contractual changes will be effected nor will any additional burdens be conferred on the Valuation Joint Board.
- There can be no presumption that any or all requests to work from home will be approved.
- Line Managers will agree any home working or agile working arrangements, subject to any formal approval that might be required by the Assessor & ERO or the Depute Assessor & ERO.

5. Home/Agile Working Requests

Employees will be required to make an application for flexible working in writing to their Line Manager using the form at Appendix 1.

On receipt of requests, the line manager should consider the various matters below and record any agreed actions prior to deciding whether or not to authorise the agile/home working proposal.

6. Home Working Assessment

The blend of home and office working can and will vary from person to person, between service functions and from time to time. In considering the appropriateness of any request, line managers should consider:

- Will the service be maintained, improved, or be more accessible to service users?
- Will business processes, technology or operational procedures need to change to accommodate new ways of working?
- Is there an understanding by the employee of the required work output and outcomes?
- What are the implications for other team members (e.g. rotas, cover arrangements, organising and planning work programmes)?
- The ability to work safely and healthily from home
- Fairness and equality
- Relevant performance related issues as already discussed as part of on-going management
- The requirement for any Equality Impact Assessment
- The effect on training requirements for/of both trainees and trainers/mentors

- Any additional cost to the Joint Board, though cost alone need not be a restriction
- Will data or information be stored and processed securely? (See later)

These factors need to be taken into consideration and the impact on different service functions may not be the same. Therefore, whilst employees will have access to the same process of consideration for agile working this may not necessarily result in the same outcome.

Where there is an agreement that agile working can be implemented, the line manager must ensure the employee is aware of local and service arrangements whilst working in an agile fashion (e.g. keeping diaries up to date, etc).

7. Agile Working

Agile working must not negatively impact on service delivery. Managers must, therefore, ensure they have systems in place to maintain suitable office cover and the level of staff available.

a) Working from home

Homeworking is where an employee undertakes their role from home for part of the time. Whilst there is no requirement for employees to work from home, nor does it form part of an established work arrangement or pattern, if an employee wishes to work (partly) from home a Health and Safety risk assessment must be completed.

b) Travel

It is important that all employees working from home manage their meeting and travel plans efficiently in order to limit unnecessary expense and, potentially, achieve environmental benefits. Conference calls/remote meetings should be considered as alternatives to travelling to meetings. Any business mileage claims will be reimbursed under the usual terms and conditions of claiming expenses and subsistence allowance.

c) Hours worked

A benefit of home working is the potential ability to work outwith standard working hours. It is important, however, that working patterns are not detrimental to health and wellbeing. Employees are responsible for ensuring that their contracted hours per week are worked and recorded via timesheets, flexi updates, or other formal means, as advised by their line manager. For the avoidance of doubt, **flexi-time should not routinely be accrued by employees working from home** and any time above the contracted hours should be agreed with the line manager in advance.

d) Contractual Base

An employee's contractual designated base, at a Valuation Joint Board office location, will remain unchanged.

8. People Management

Agile working arrangements will require a different approach to direct people management, supervision, team interactions, and the nature of working relationships and communications will change. It is, therefore, essential that everyone within the team co-operates and there is a high

level of trust and confidence between the line manager and employees. **Arrangements will be put in place to monitor work output, performance, communication, and support**.

The agile worker must be a motivated individual who is also in a position to undertake work which requires minimal immediate input from their supervisor or line manager. However, line managers should establish clear arrangements for:

- Setting clear objectives, work programmes, and targets in relation to work completed;
- Implementing procedures to monitor performance, outputs, and hours worked;
- Encouraging employees to analyse and understand their workload and how it will be delivered;
- Encouraging everyone to take more responsibility for managing their time and organising their workloads;
- Ensuring effective formal and informal communication across the entire team including regular team meetings, one-to-one sessions, training, and email;
- Maintaining agreed contact levels with team members;
- Regularly checking that team members receive enough support; and
- Being alert, recognising, and addressing any difficulties as they arise.

a) Attending the office

Agile workers are required to attend their normal office for team meetings, training and development, one to one meetings, and any other event as required by their line manager. Home working options may have to be withdrawn at peak and/or busy periods.

b) Communication

It is essential that the regular forms of organisational communication are accessed and used by the agile worker. While working away from the office, appropriate telephone calls and email forwarding or messaging should be in place and calendars updated and accessible to enable review of appointments and whereabouts. In addition, employees should be contactable via a mobile phone (personal or work) or other approved collaboration tools at all times during contracted/agreed working hours.

9. Health and Safety

The Joint Board has a duty of care to protect all employees. However all employees must exercise reasonable care for themselves and others while carrying out their responsibilities, regardless of location. Agile working at home will be low risk type of work, however, relevant Home Health and Safety assessments (see Appendix 2) must be undertaken before any employee is able to work in an agile way. All Health and Safety Guidance must be referred to in order to support this process.

Managers should ensure that, together with employees, health and safety assessments are reviewed at least annually or when any changes are made to the employee's workspace or work style. A Display Screen Equipment (DSE) self-assessment will require to be completed by all employees.

If an employee does not have the appropriate facilities or support available to work safely from home, the employee will not be allowed to do so and will need to work from their contracted base.

Employees who have any concerns relating to health and safety aspects of their work should inform and discuss these with their line manager, and certainly prior to any request for home working.

10. Technology and Equipment

The line manager will be required to establish any technology requirements which may include the issue of mobile devices or the use of desktop equipment.

Where a Joint Board PC, laptop or mobile device has been provided to an employee, it must be noted that this has been allocated for business use only.

In order to access work e-mails or corporate systems remotely, employees require secure access via Netscaler and the ability to connect to the internet. Employees will be responsible for providing internet broadband, of a suitable speed and consistency of service, in their homes.

Where employees have their own personally adapted equipment (e.g. left hand keyboard, mouse, wrist support, etc) they will move it with them when working from home. However, where an employee is not able to transfer their specially adapted equipment and potentially cannot work safely from home, further HR and Health & Safety advice should be sought prior to approving home working.

The Joint Board's ICT security policies can be found on the appropriate shared network drive.

11. Data Protection and Security

All Joint Board policies and procedures relating to data protection, security, and confidentiality are equally applicable within an office base or at home. In general, employees must ensure:

- appropriate care of equipment, access to systems, files, and any other information;
- that unauthorised people cannot view or access confidential or personal information;
- that all Joint Board paperwork and equipment is held safely and only accessible to the employee, including during transportation;
- that screens and documents cannot be readily overlooked when working from home;
- that any Joint Board equipment transported in a vehicle is locked away and, where possible, out of sight;
- no documents or information are copied to an employee's personal devices.

Employees could be held liable for breaches of the Data Protection Act if appropriate security measures have not been taken, by the employee, to safeguard personal data and comply with the Joint Board's ICT security policies. Further information on information and data security requirements are contained in Appendix 3 to this Guidance.

Any data loss or data breach must be reported immediately to the line manager or Assessor / Depute Assessor

12. Training

West Dunbartonshire Council's Organisational Development and Change team offer a workshop to support Line Managers in managing a flexible team effectively. Contact OD & Change for support.

13. Review

It is essential that managers and employees, alike, adopt a shared ethos to agile working within the boundaries of normal service provision. It is recognised that a 'one size fits all' approach cannot be applied and any agile working arrangements will be regularly reviewed.

Where there is a change in service provision, service user requirements, or employee circumstances, the line manager has the right to end any arrangement with reasonable notice. In addition, any agile working arrangements should be reviewed at least annually. Where a line manager feels that agile working is no longer in the best interest of the Joint Board or the employee, the arrangements will cease.

14. Responsibilities

Line Manager Responsibilities:

- Ensuring that the agreed process is complied with and that it is effectively, fairly and consistently applied within their areas of responsibilities.
- Ensuring that all employees are made aware of their responsibilities in relation to HR, Health and Safety, ICT and Data Protection.
- Ensuring that they discharge their duties in relation to health and safety for any employees for whom they are responsible, including health and safety assessments, providing required equipment; and acting on any areas of concern.
- Having joint responsibility with employees to come to an agreement on working in an agile way and how this will be done.
- Being flexible, open and constructive in relation to discussion and agreements about agile working whilst remaining focussed on the needs of the service.
- Agreeing appropriate contact arrangements for any employee who undertakes agile working and ensuring the employee attends team meetings as required.
- Ensuring that defined performance objectives are set and reviewed during Performance, Development and Training Reviews and at all times.

Employee Responsibilities:

- Working within these guidelines in a reasonable, constructive, and appropriate way.
- Having joint responsibility with managers to come to an agreement regarding working in an agile manner and how this will be done.
- Being flexible, open and constructive in relation to discussions and agreements about agile working whilst remaining focussed on the needs of the service.
- Being responsible for working within agreed "protocols".
- Having a responsibility to comply with health and safety requirements, participate in/ undertake appropriate self-assessments and carry out necessary actions to minimise risk and maintain a safe working environment.
- Ensure that the home work space is safe and complies with Health and Safety requirements. Home working staff remain responsible for the reporting of any H&S breaches to management.

- Adherence to the requirement of Joint Board policies, including HR, Health and Safety, ICT and Data Protection (See Appendix 3).
- Compliance with the Code of Conduct duty to take all reasonable care to ensure the security and condition of equipment and data in their care.
- All employees must ensure they are able to attend Joint Board offices when requested to be present at meetings or other events.

Dunbartonshire and Argyll & Bute Valuation Joint Board

APPENDIX 1

Request for Agile Working Application Form

Employees should complete page 1 and pass the application to your line manager

Employee details			
Surname		First name(s)	
Designation		Employee ref	
Date		Section/ Location	

Confirm your current working pattern (days/hours/times worked)
Confirm the home working pattern you would like to work in future (days/hours/times worked)
Date you would like this to commence

I have read the DAB VJB Agile Working Guidance and I am aware of my responsibilities in respect of:

- **The requirement to complete a Home Working Assessment**
- **The requirement to complete Health & Safety (including Display Screen) Assessment**
- **Care of all Joint Board equipment, hardware and ancillaries**
- **Information and Data Security**

Signed	**Date**

When completed this form should be submitted for consideration to your line manager.

Request for Agile Working Application – Line Manager Assessment

Line Managers should record any issues arising from the Home Working Assessment under each heading below and confirm any Action agreed with the employee.

	Issues Arising	Agreed Action
Service Provision		
Performance		
Home Working Assessment		
H&S Assessment		
ICT		
Training Requirements/ Responsibilities		
Data Information & Security		
Additional Cost to VJB		
Other		

I have considered all issues as identified in the DAB VJB Agile Working Guidance and approve/reject (delete as appropriate) **this application.**

Line Manager…….. **Date ……**

APPENDIX 2

REMOTE WORKING SELF ASSESSMENT CHECKLIST

ASSESSMENT DETAILS			
Name of remote worker		**Date of assessment**	
Address		**Date of review[1]**	
Work location / room		**Name of line manager**	
Signature of remote worker		**Signature of line manager**	

REMOTE WORKING ACTIVITIES			
Summary of work activities carried out at home			
Equipment Used			
Employer Provided		**Remote worker's Own**	

The employee must provide a photograph of their workstation as part of DSE assessment to ensure suitability

The checklist will be completed by the employee and sent to the line manager for review and action. The DSE assessment (which forms part of the checklist – see https://west-dunbarton-dash.achieveservice.com/service/DSE_Employee_Questionnaire) will also be completed by the employee. The line manager will be responsible for progressing any actions arising from the assessment.
The assessment should be reviewed in the event of any significant changes to the nature of work carried out, equipment used or the work environment and, in any case, at regular intervals. The remote worker must inform the employer without delay where any significant changes occur.

REMOTE WORKING EMPLOYEE SELF–ASSESSMENT CHECKLIST AND ACTION PLAN

No	Question	Y / N or N/A	Employee's Comments	Further Actions Required	Actions Completed (person and date)
1. DISPLAY SCREEN EQUIPMENT (DSE)					
a	Does the work involve significant use of DSE?				
b	Has a DSE Self-Assessment been completed?				
2. WORK LOCATION					
a	Is the work area segregated from normal living areas and other occupants of the house?				
b	Are there any obvious hazards / risks associated with other activities / personnel within the house?				
3. ENVIRONMENT					
a	Is natural lighting utilised where practicable?				
b	Are lighting levels adequate, including any necessary task lighting?				
c	Does lighting / windows cause glare?				
d	Is a comfortable temperature maintained without draughts?				
e	Are noise levels comfortable?				
f	What are the conditions of the floor coverings and any defects identified?				
g	Are walkways clear of tripping hazards e.g. trailing cables				
h	Are there any slip / trip hazards or unacceptable obstacles				
i	Is there adequate working space and sufficient safe storage?				
j	Is there adequate ventilation?				
4. ELECTRICAL					
a	Is the fixed electrical system (sockets, wiring etc.) in good repair?				
b	Is all electrical equipment provided by the employer 'PAT tested?				
c	Is there any damage to leads or plugs etc.?				
d	Is any equipment provided by the remote worker in good				

	repair, any damages to leads or plugs etc.?				
e	Does the remote worker carryout pre-user checks/inspections on the electrical equipment being used?				
f	Does the remote worker know how to inspect equipment for electrical safety and how to report faults?				
g	Are cables secure in all plugs?				
h	Are there sufficient sockets and no socket overloading?				
i	Are cables untangled, in good repair and not trailing?				
5. FIRE					
a	Are there any uncontrolled ignition sources?				
b	Are combustible materials and waste materials minimised?				
c	Are waste materials regularly disposed of and how often?				
d	Is there a smoke detector/alarm fitted in the work area?				
e	Does the remote worker know what to do in the event of a fire?				
f	Is there a means of raising the alarm or calling for assistance?				
g	Are all exit routes clear of obstruction?				
6. PSYCHOLOGICAL RISKS					
a	Is isolation likely to be a significant issue?				
b	Is the employee aware of and fully conversant of the Joint Board's Policy on Managing Stress?				
c	Is workload manageable and properly managed?				
d	Is communication with the line manger adequate?				
e	Is adequate support from colleagues / Management available?				
7. MANUAL HANDLING					
a	Does the work involve significant manual handling or raise ergonomic concerns?				
b	Has a manual handling assessment been carried out?				
8. SECURITY					
a	Do the house / working environment / activities carried out raise significant security concerns?				

b	Is the final exit door securely locked?				
c	Do all operated windows securely closed/locked?				
d	Can laptop and files be securely locked away when not in use?				
9. ACCIDENTS AND INCIDENTS					
a	Does the remote worker know the procedure for reporting any accidents, incidents, near misses or work related illness?				
b	Is the remote worker aware of how to deal with accidents or incidents?				
c	Is a first aid kit available at home?				
10. COMMUNICATION					
a	Are adequate arrangements in place for the remote worker to report to their line manager regularly?				
11. EQUIPMENT					
a	Is any equipment used which presents a risk (and, if so, is all guarding / controls etc. in place)?				
12. INFORMATION, INSTRUCTION, TRAINING					
a	Have all mandatory health and safety e-Learn modules contained within Core Training been completed?				
13. OTHER HAZARDS / RISKS					
a	Does the remote worker suffer from any discomfort or ill health that they believe has resulted from their work?				
b	Does the remote worker suffer from any allergies that may affect them as a home worker?				
14. ANY OTHER COMMENTS YOU HAVE REGARDING THE HOME WORKING ENVIRONMENT:					

Appendix 3

Home and Flexible Working Information and Data Security Guidelines

Audience and Scope

This guidance is intended for all staff that work at home or any other locations (meetings, survey etc) either on an occasional or a regular basis. This guidance relates to all information held in any format, including paper files, electronic data, including word processed documents, website published data and emails. This guidance is aimed, in particular, at anyone who processes personal data, sensitive business information or confidential information. Some examples of what constitutes high or medium risk personal data or sensitive business information can be found later in this document.

This guidance gives general advice on the issues you need to consider to ensure that any information you work on out-with your normal office environment is protected from loss or unauthorised access and exploitation, while at the same time ensuring that it is accessible to anyone that needs to use it for work related purposes.

What Do I Need to Do?

Taking personal information out-with the office will always involve an element of risk so you should think carefully about whether you need to do so. The measures you take when working at home or remotely will depend on the nature and sensitivity of the information involved, and should take into account the consequences of someone else gaining access to the information.

The guidance is divided into sections that apply to information in all risk categories and others which apply to high or medium risk information.

This guidance document applies specifically to work that you do at home or in remote locations. You should always limit the need to take information home by connecting directly to the Joint Board servers using remote access facilities, but if you remove information from the Joint Board environment you must adhere to the guidelines.

Guidance for all categories of information

Key Principles

The following key principles underpin the Joint Board's guidance on the storage, transmission and use of **all** data and information outside Joint Board offices. All staff must comply with these principles when using mobile devices and portable storage media or otherwise removing (or capturing) information outside the Joint Board offices.

The overarching principle is that employees are responsible for protecting information, including personal information in the ownership of the Assessor & ERO or the Joint Board. This applies whether the information is held/processed on computer, or in paper records, and whether the information/device is used in the workplace, at home or at other locations. Employees must understand that this is a key element of home working and must make every effort to ensure the safety and security of all data and information at all time.

Wherever reasonably possible, information should be:-

- Kept in a locked filing cabinet, drawer, cupboard or room, whether it is in paper or electronic format, when not being worked on or when the location is left unattended (even for a short time).
- Not visible, either on desks or on computer screens, to anyone not authorised to see it — ensure screen savers and computer screen locks are used

- Contained in a sealed envelope, if transmitted through the mail, either internally or externally
- Not sent via e-mail if it is sensitive information unless encrypted email is used or this is done via a secure network
- Not disclosed orally or in writing without the permission of the service user or staff member unless it is part of a legitimate process
- Locked away in the boot/out of sight whilst when transporting the information by car
- Kept in a secure/locked bag when travelling on public transport

Other security issues to be considered include:-

- Avoid removing personal, sensitive or confidential data from Joint Board premises wherever possible.
- Only encrypted devices provided by the Joint Board should be used to work from home.
- If the use of personal data is unavoidable, consider partially or fully anonymising the information to obscure the identity of the individuals concerned.
- Use the Joint Board's secure shared drives to store and access personal data and sensitive business information, ensuring that only those who need to use this information have access to it.
- Use remote access facilities to access Joint Board systems, personal data and sensitive business information on the corporate network instead of transporting it on mobile devices.
- If there is no option but to use mobile devices, use encryption software, or encrypt the whole hard disk/device.
- Do not use personal equipment (such as home PCs or personal USB sticks) or third party hosting services (such as Google Mail or Dropbox) for personal data or sensitive business information.
- Avoid sending personal data or sensitive business information by email. If you must use email to send this sort of data outside the Joint Board, encrypt it. If you are sending unencrypted high or medium risk personal data or sensitive business information to another Joint Board email account, indicate in the email title that the email contains sensitive information so that the recipient can exercise caution when opening it.
- Where sending personal data out-with the Joint Board ensure that the requirements of any relevant data sharing agreement are complied with.
- Do not use personal data or sensitive business information in public places. When accessing your email remotely, exercise caution to ensure that you do not download unencrypted personal data or sensitive business information to an insecure device.
- Implement the Joint Board's retention and disposal policies so that you do not keep data and information that you do not need. If there is no suitable retention and disposal policy in place for that particular piece of information please consult with your line manager.
- Inevitably, there will be occasions when data will be transferred from one area of the organisation to another. Where the transfer of personal data occurs, the transfer must be reasonable and legitimate (taking into account the initial reasons for the collection of the personal data in the first place).

Working from Home

Encrypted Joint Board devices should be used when working from home. All information should be stored on the Joint Board computer network. Wherever possible, you should work directly from / to the appropriate Joint Board servers using remote access facilities.

Your Joint Board device will be setup to ensure that the computer operating system and applications are up to date with virus protection software and any relevant security patches.

Direct access to Joint Board systems should reduce the need to take paper information home.

If you must take personal information outside the normal Joint Board environment to your home, adhere to the following rules:

- Your work area should preferably be in a separate location to general 'living' areas. This location should not be able to be easily seen or accessed by people outside the home. For example, you should not situate your work area or computer station next to a ground floor window.
- Make sure that information is not left where other occupants of your home can easily see it.
- Keep paper documents, files and portable encrypted media or devices containing information in a lockable cabinet wherever possible and make sure that this is locked when not in use.
- Wherever possible, physically protect laptops. You may do this by using a lock or cable to secure the laptop, or placing it in a locked cupboard or drawer when not in use.
- If you are taking sensitive information home, in any format, go there directly. This reduces the chances of losing the information on the way.
- Use an appropriate carrier. Documents, portable encrypted media and devices should be transported in a secure, briefcase or bag.
- Exercise discretion. Do not read sensitive documents on a bus, for example, or work on personal data on a train. Do not draw attention to the fact that you are carrying Joint Board information.

Working Away from Your Normal Environment

If you have to take Joint Board held information home or to a remote location, always use an encrypted Joint Board provided laptop or PC.

If you must take paper documents then only take the paperwork necessary to carry out your task. Ensure that you note/record the paperwork that has been taken out the office.

- Joint Board records should be updated as soon as possible with any work that you do at home.
- Security should be of an equivalent standard to that which is provided in Joint Board offices.
- See above regarding transporting information and data away from the workplace.
- Avoid leaving files in public lockers in, for example, train or bus stations.

Destruction of Personal or Confidential Data

The measures you take will depend on the data involved. Reference should be made to the Joint Board's Records Retention Schedule and Data Destruction Policies at all times.

Personal or Confidential information must be disposed of using the confidential waste facilities provided by the Joint Board. Domestic shredders or waste facilities must not be used.

Guidance for High Risk Personal Data or Sensitive Business Information

High risk information should only be removed from the office by staff who need to use it away from Joint Board premises as a necessary part of their job.

If using high risk information away from the Joint Board, the guidance provided above should be read as being instructive and should be adhered to. If you need to carry information with you out with your office, by preference, return it at the end of your working day to store it securely, rather than taking it home. If you do take it home, ensure that you are able to lock the information away securely at home.

Do not use your own, non-Joint Board, PC, laptop or other device to store sensitive Joint Board information. This is non-negotiable, only use a Joint Board provided encrypted device.

The following are examples of high risk personal data or sensitive business information:

- Any bulk data sets relating to 1000 or more identifiable individuals, including, but not limited to, staff or service users.
- Any data sets relating to identifiable individuals that could be used for fraud or identity theft, including, but not limited to, bank account or credit card details, national insurance number, personal contact details, date of birth and salary.
- Information relating to individuals performance, grading, personal and family lives.
- Any set of data relating to an identifiable individual's health, disability, ethnicity, sex life, trade union membership, political or religious affiliations or the (alleged) commission of an offence.
- Substantial reorganisation or restructuring proposals that will have a significant impact on employees/individuals before relevant decisions are announced.
- Discussion papers and options relating to proposed changes to Joint Board strategies, policies and procedures before the changes are announced.
- Security arrangements for high profile or vulnerable visitors, clients or staff, events or buildings while the arrangements are still relevant. This includes door access codes and passwords for access to the Joint Board network or other key systems.
- Non-public data that has the potential to seriously affect any organisation's commercial interests or the Joint Board's corporate reputation.
- Information obtained under a confidentiality agreement or statutory power where disclosure of the information is likely to seriously affect the Joint Board's reputation or lead to an action against the Joint Board for breach of confidence.
- Information that, if compromised, would substantially disadvantage the Joint Board in commercial or policy negotiations.

Why do the Data Protection and Freedom of Information (Scotland) Acts affect me when I work at home?

The Data Protection Act 2018 and the Freedom of Information (Scotland) Act 2002 apply to all paper and electronic information that you create and receive as part of your employment with the Joint Board, regardless of where you work or store that information.

The Data Protection Act sets out how organisations can handle personal data and gives an individual the right to access personal information held about them.

The Freedom of Information (Scotland) Act entitles anyone from anywhere in the world to request access to any information held by the Joint Board. It also includes a statutory code of practice on records management which describes the systems we should have in place for managing our information.

These pieces of legislation are as applicable to work you do at home as work you do on Joint Board premises, so you must therefore take this guidance into account when working at home.

Consequences of Non-Compliance

Failure to comply with this guidance could expose the Joint Board, its staff or citizens to risks including fraud, identity theft and distress, or damage the Joint Board's reputation and its relationship with its stakeholders, including citizens.

A failure to safeguard personal data at home could breach the Data Protection Act 2018, which could lead to the Assessor, the ERO and/or the Joint Board being fined up to €20,000,000. The Information Commissioner, who regulates data protection, takes the loss of data through flexible working seriously – significant fines have been issued for the loss of laptops by organisations. The loss of important information could also impact on the operation of the Joint Board, for example, by losing the only copy of financial information.

The Data Protection Act 2018 sets out how organisations may use personal data. It states, "**Appropriate security of the personal data, using appropriate technical or organisational measures including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage”**.

This requirement involves a judgement as to what measures are appropriate in particular circumstances. This guidance provides information for Joint Board staff on how to make this judgement when using, transporting or storing personal data or highly sensitive information outside the Joint Board.

Following the guidelines enables you to confidently access the information you need to do your job and safeguards your information against loss, theft and corruption.