MERTHYR TYDFIL
County Borough Council
Cyngor Bwrdeistref Sirol
MERTHYR TUDFUL

Merthyr Tydfil County Borough Council

Remote Working Policy

Issue Date	**Version**	**History of Changes**	**Approval**
22/05/2013	1.0	No policy changes.	ICT Security Forum
25/02/2014	2.0	No policy changes.	ICT Security Forum.
05/08/2014	3.0	Implementation Responsibilities updated to reflect IGF responsibilities.	Information Governance Forum.
11/03/2016	4.0	User responsibilities updated (1.2, 1.3, and 1.4).	Information Governance Forum
16/03/2017	4.0	No policy changes	Information Governance Forum
06/02/2018	5.0	Reference to DPA98 removed and updated with relevant DP Laws.	Information Governance Forum
27/09/2018	6.0	DPA Policy in 3.1 amended to Privacy Standards Policy	Information Governance Forum (IGF)
18/10/2019	6.0	No policy changes – approved	IGF
13/11/2020	7.0	Policy updated in line with new Agile ways of working. Appendix 1 and 2 also added.	IGF

Remote Working Policy

Objective

This policy shall apply to all Merthyr Tydfil County Borough Council (MTCBC) employees, Members and third parties who engage in remote working. The objective of the Remote Working Policy is to ensure the effective and appropriate use of MTCBC ICT equipment when used out of the main office. While MTCBC is committed to remote working for business purposes, it must ensure that suitable controls are in place to prevent security breaches or other negative consequences.

This policy has been developed to manage the way in which the authority complies within the ISO 27001 standard.

Scope

This policy applies to all employees, Members and third-parties (referred to as 'users') who use MTCBC ICT facilities and equipment remotely, or who require remote access to MTCBC information systems or information.

Policy Statements

MTCBC provides users with the facilities and opportunities to work remotely as appropriate. MTCBC will ensure that all users who work remotely are aware of the acceptable use equipment and remote working opportunities.

This policy must always be adhered to whenever any user makes use of MTCBC ICT equipment when working on Council business away from MTCBC premises.

Implementation Responsibilities

The Information Security Officer shall develop, maintain, and publish processes to achieve compliance with this policy. Any queries can be directed to 01685 727444 or via email, information.security@merthyr.gov.uk .

All Heads of Service shall be responsible for implementing the Remote Working Policy within their areas of responsibility.

All ICT equipment supplied to users is the property of MTCBC. It must be returned upon the request of MTCBC. Access for ICT Services staff of MTCBC shall be given to allow essential maintenance, security work or removal, upon request.

All ICT equipment will be supplied and installed by ICT, hardware and software **must only** be provided by MTCBC.

The method for users' remote access to the network must be supplied and managed by MTCBC ICT Department.

All employees, Members and third-parties (known as 'users') shall sign the Information Security Policy to indicate their agreement to comply with the Remote Working Policy.

The Information Governance Forum are authorised to update and amend the Information Security Policy and this supporting operational policy following consultation with the Portfolio Member for Governance and Corporate Services.

1. User Responsibility

It is users' responsibility to ensure that the following points are always adhered to:

1.1.1 Users must take due care and attention of ICT equipment, devices and paper files when moving between home and another business site, as well as moving between business site to business site. ICT equipment and paper documents should be stored out-of-sight in the boot of a car when travelling between office sites and/or home; Information must be kept secure and a briefcase, laptop or paper documents must never be left unattended.

1.1.2 Departments must have in place procedures for staff to sign out paper documents classified PROTECT or above (see Information Asset Protection Policy for the Council's Information Handling Guidelines) when these are being taken out of the office to work at home.

1.1.3 Paper documents removed from the office to work at home must be returned to the office as soon as there is no longer a business requirement to retain them at home and must be signed back in as soon as they are returned to the office.

1.1.4 At home, personal data in paper format must be stored securely and separately from any ICT equipment such as PCs, laptops, or tablets e.g. papers should be stored together in a bag or box away from other members of the household.

1.1.5 Paper documents removed from the office and taken home must be returned to the office for destruction immediately after use. Staff must not destroy Council information unless they have been provided with a suitable shredder by the Council.

1.1.6 It is the duty of the user working at home or outside of the office to take all reasonable precautions to protect information relating to their employment.

1.1.7 Information which contains data about any identifiable living individual is subject to relevant Data Protection Laws. Users working at or from home need to know and understand their obligation to keep data confidential and secure.

1.1.8 Users will not install or update any software on to Council owned ICT equipment or device.

1.1.9 Users will not install any screen savers on to Council owned ICT equipment or device.

1.1.10 Users will not change the configuration of any Council ICT equipment or device.

1.1.11 Users will not install any hardware to or inside any Council owned ICT equipment or device.

1.1.12 All faults must be reported to the ICT Helpdesk. Any Information Security issues MUST be reported to the Information Security Officer without delay via information.security@merthyr.gov.uk or 01685 727444.

1.1.13 Users must not remove or deface any asset registration number.

1.1.14 User requests for upgrades of hardware or software must be approved by a Manager via the electronic 'ICT Request Form'. Equipment and software will then be purchased and installed by ICT Services.

1.1.15 Only software supplied and approved by MTCBC can be used.

1.1.16 No family members may use the ICT equipment supplied. The ICT equipment is provided for the staff members' sole use and to be used for work Council business only.

1.1.17 The user must ensure that reasonable care is taken of the ICT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of any of the above, MTCBC may recover the costs of repair.

1.1.18 The user should not take their supplied ICT equipment outside of the UK.

1.1.19 ICT Services may at any time, and without notice, request a software and hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.

1.1.20 No user should undertake work at home or remotely using their personal ICT equipment and must understand that they are not permitted to hold any database or information relating to MTCBC, its employees or customers on personal ICT equipment. The only time users will be permitted to use personal ICT equipment for remote working is if the ICT Department has provided the technology to work remotely using strong authentication solutions. **Under no circumstances** should information classified PROTECT or above be emailed to a private/personal non-Council email address. (For further information please refer to the Email AUP and Information/Asset Protection Policy). If a user has a requirement to work remotely then they should contact the ICT Department so that a suitable solution can be put in place.

1.1.21 When working at home, users must pick a place that is private. It is important that your computer screen is kept private. This is particularly important if you handle sensitive or personal information.

1.1.22 If you are having conference calls or video meetings, be aware of other members of the household being able to overhear. A simple solution is to close the door of the room you are working in, essential when dealing with personal information.

1.1.23 Make sure that digital home assistants like Alexa are turned off before you start work.

1.1.24 Be alert for phishing emails. Criminals try to take advantage of fear and uncertainty. Never click on a link or attachment you were not expecting, even if it appears to be from somebody you know.

1.1.25 Always lock your laptop (Ctrl-Alt-Del) when you leave your workspace.

1.1.26 Keep the laptop safe when you are not using it.

1.1.27 Do not attempt to disable or bypass any security settings on your laptop e.g. anti-virus/Windows update settings.

1.1.28 Do not deface the laptop e.g. attaching stickers or use it in a way that is likely to cause damage e.g. putting a drink on the laptop. Damaged laptops that cannot be re-issued may be chargeable to your department.

1.1.29 Do not leave your laptop in a vehicle overnight.

1.1.30 Do not attach or connect unauthorised or personal USB, wireless or Bluetooth devices, including personal mobile phones to your laptop.

What personal devices can I connect to my laptop?

2.

✓  **Monitors / TVs – either wired or wireless**

✓  **USB mice / keyboard**

✓  **USB wired Headsets**

✓ **Printers**

*What personal devices can I **NOT** connect to my laptop?*

✗  **USB / Bluetooth Smart Speakers including digital assistants**
like Amazon Echo and Google Nest.

✗ **Wireless Bluetooth Headsets and earphones:** Wired headsets only are permitted.

Electric cigarettes / Vapes: do not connect devices to your laptop to charge them.

USB novelty items such as Christmas lights, desk fans, cup warmers.

Jigglers: These devices connect to your laptop and are designed to keep your screen active by randomly moving your mouse. They can also give the appearance that you are active on your laptop when you are not (e.g. Microsoft Teams status).

Mobile phone: Only charge your work phone in an emergency if a 3-pin plug is not available. You may not charge any other items from your work laptops. Personal mobile phones must not be connected to laptops or docks.

Memory sticks / hard drives: While you have read-only access on your laptop, under no circumstance should you connect memory sticks / hard drives from unknown sources as these could be malicious. USB read access is only allowed for memory sticks / hard drives that have been approved for business use.

2 Remote and Mobile Working Arrangements

Users must be aware of the physical security dangers and risks associated with working within any remote office, at home or mobile working location:

2.1.1 Equipment should not be left where it would attract the interests of the opportunist thief, in the home it should be ideally located out of sight of the casual visitor.

2.1.2 Users must ensure that passwords are not written down and left in the area of MTCBC ICT equipment (see Password Policy for further information).

2.1.3 All paper documentation should be securely locked away and a clear desk maintained outside of working hours (See Clear Desk Policy for further information).

2.1.4 Wastepaper containing PROTECT (or above) classified information must be shredded using a security level 4, cross-cut shredder as a minimum standard. The Print Department provide a shredding service, and lockable secure storage bins are placed next to the photocopiers in Civic Centre and Unit 5 for shred waste to be disposed of.

2.1.5 PCs/laptops/tablets should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

2.1.6 Users who have access to their corporate emails on a personal device via Blackberry Work or Office 365, must IMMEDIATELY notify the ICT Department (Tel. 01685 72(5450) or helpdesk@merthyr.gov.uk) if their personal device is lost or stolen. In the event of theft or loss of a users' personal device, the ICT Department will remotely wipe the app from the device to avoid unauthorised access to corporate emails.

2.1.7 Microsoft Teams is an integrated communications tool capable of Instant Messaging (IM), voice calls and video between one or more participants. Your contributions to video calls and instant messages are in scope of Freedom of Information requests and Data Protection Legislation. Remember, any participant (internal or external) may have taken a copy of the call/messages.

2.1.8 Your photograph on Microsoft Teams will not be displayed by MTCBC, however, you have the option of adding a photo of yourself to your bio. Your photograph must be a true likeness of yourself e.g. pictures of celebrities, cartoons, places are forbidden.

2.1.9 You may share a single application at a time via Microsoft Teams with other participants e.g. to show them a document or a presentation. You must not give control of your screen to an external participant.

Further guidance regarding the use of Microsoft Teams can be found in Appendix 2.

3.0 User Awareness

The Council has policies about information management and relevant Data Protection Laws in place which should also be considered in remote working and home-working arrangements. All staff must comply with appropriate policies associated with the use of ICT equipment. This includes the following:

- Email & Instant Messaging AUP
- Clear Desk Policy
- Internet AUP
- Password Policy
- Information Backup and Storage Policy
- Physical Security Policy
- Reporting Information Security Events
- Software Compliance AUP
- Social Media Policy (separate policies are in place for employees and Members)
- Telephones, Secure Printing and Facsimiles Policy
- Unauthorised Access Policy
- Antivirus Policy
- Information/Asset Protection Policy
- Disposal of ICT Equipment Policy
- Privacy Standards Policy

It is the staff member's responsibility to ensure their awareness of and compliance with these policies.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Information Security Officer, 01685 727444, information.security@merthyr.gov.uk .

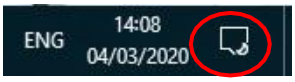
Appendix 1 – Connecting to the MTCBC network from home

There are two easy steps that will enable you to connect to the MTCBC network from home. You need to connect to your Wi-Fi network within your home (if you have one) and then connect to the MTCBC network via Global Protect.

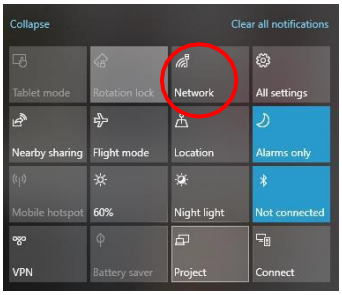
If you do not have Wi-Fi at home, you can use your mobile phone to create a personal hotspot but please be aware that this uses your data allowance quickly. It is not advisable to create a personal hotspot unless you have a corporate phone or have unlimited data on your personal phone.

Connecting to your home Wi-Fi

1) Click on the action/notification centre in the bottom right-hand corner of your laptop screen



2) Your notification centre will open. If you only have 4 squares click on 'extend' above the 'tablet mode' button. Click on Network.



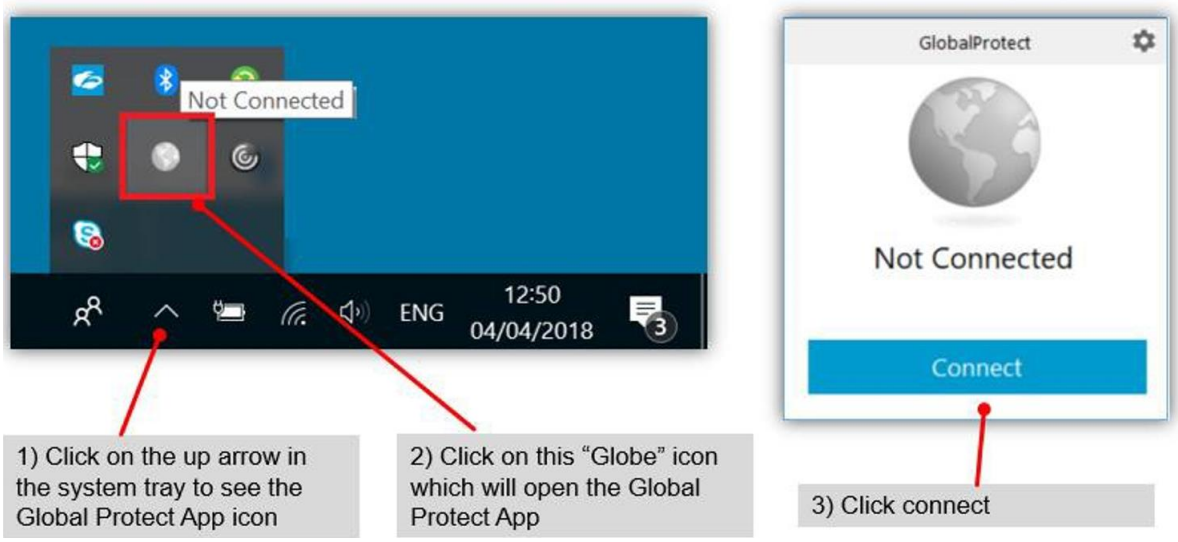
3) A list of available networks will appear. Your home network (or personal hotspot) will be one of them. Click on the network you wish to connect to. You can leave the 'connect automatically' box ticked. You may be asked for a password/passkey. This will have been provided by your broadband provider (and is usually found on the back of your home router) when your broadband was set up (or there will be a password provided on your mobile to connect to your personal hotspot).

Connecting to Global Protect

The Global Protect app allows you to connect to the MTCBC network when you are working away from the office. To connect you must authenticate using your username and password (these are the credentials that you use to log on

to your laptop).

Ensure you are connected to Wi-Fi, follow the instructions below to log into the MTCBC network:



You will then be prompted to enter your username and password. After this, you will be connected to the MTCBC network via Global Protect.

Trouble Shooting Tips

If you are having difficulties connecting through Global Protect, please contact the ICT Helpdesk but the following may also resolve any difficulties you are experiencing.

 Ensure you have a Wi-Fi connection. Search for a website or check that the little Wi-Fi symbol shows a good signal (the number of lines showing in white indicates the strength of your Wi-Fi signal)

 If Global Protect keeps telling you it is connecting but you cannot access corporate applications, click on the three little lines on the top corner of your global protect window.

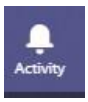
Click on **Refresh Connection** and it should then ask you to sign in again with your password and attempt to re-connect.

Sometimes Global Protect gets caught in a continual loop – the application keeps asking you to sign in despite you having already tried to do so. Try to Refresh the Connection and if that does not work after a couple of attempts please contact the ICT Helpdesk. They will be able to see why you are unable to connect and resolve it for you i.e. there is a sync issue, or your account has temporarily locked itself.

Appendix 2 – Microsoft Teams

You can open Microsoft Teams by clicking on the icon on the desktop or by searching 'Teams' within Cortana.

The following can be accessed from the task bar within Teams on the left-hand-side of the application's Window:



Creates a summary of activity – calls made, where people have specifically mentioned you in chat.

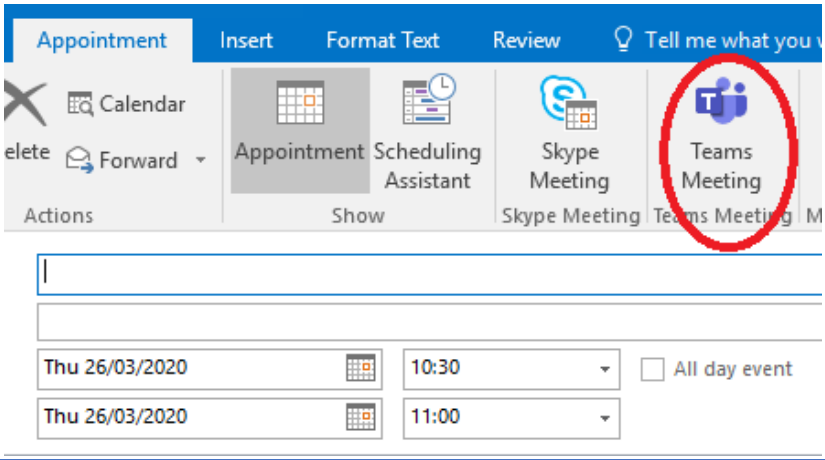
Instant Message feature

Displays the same information as your Outlook calendar – any meetings made within Teams will also show in Outlook and vice versa (please note that only those users with an E3 Microsoft Office 365 licence will see their Calendar in Microsoft Teams)

Create a Teams meeting

You can schedule a Teams meeting in the same way that you schedule a calendar appointment in Outlook.

1) Open Outlook and create a new meeting in the normal way and invite attendees



2) Before you send your invitation, click on the **Teams Meeting** button.
3) Notice a **Join Teams Meeting** link has been inserted in the message area.
4) Enter any further text in the message area and send.

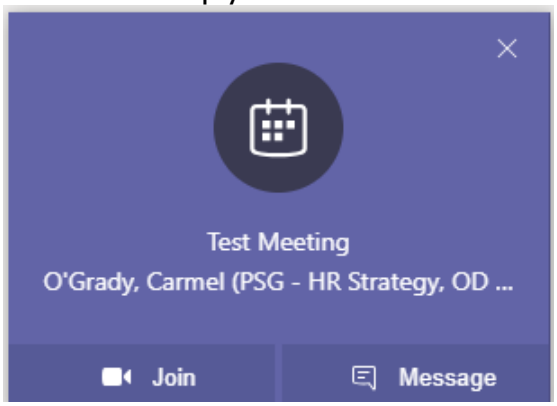
Add a Teams link to an existing meeting.

If you need to add a Microsoft Teams link to an existing meeting, open the meeting invitation and then click on the **Teams Meeting** button (as above) and a 'Join Teams meeting' message will drop into your existing meeting invitation. You can then resend to meeting participants.

Join a Teams meeting

If you have been invited to a Teams Meeting you can join in three ways.

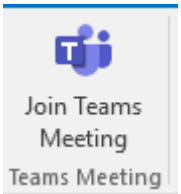
1. You can simply click **'Join Online'** when you receive your 15-minute



reminder

2. You can click on the Teams link from within the calendar invitation and accept the defaults to join the meeting:

3. You can also open the meeting invitation and click '**Join Teams Meeting**' button in the menu bar.



You can then follow the onscreen instructions.

Meeting Etiquette

When everyone is not in the same room, meetings may require a bit more planning. Below are some suggestions to help you and your team:

- Use a headset with microphone to help ensure good audio quality during the meeting. You can order them via the ICT Department, or you are able to use your own if you prefer (N.B. headphones must be connected via cable
- (headphone jack or USB), do not use Bluetooth or wireless headphones or speakers.
- When you send out the invitation or agenda, make sure you are clear on etiquette – e.g. phones on silent, use of laptops, microphones on mute when you are not speaking etc.
- The Chair should remind all attendees of the protocols around phone use etc at the beginning of the meeting.
- Laptops can be helpful in some meetings – even if you attend using Teams, you can still take notes and reduce the need to print by looking at papers electronically. However, attendees should be focused on the topic of the meeting, not doing other work, or responding to unrelated emails.
- Make your presence known, the Chair should always ask remote attendees whether they have anything to raise or make sure they have understood any decisions before moving on to the next agenda item.
- Make sure you let the Chair know whether you can hear others clearly. If there are any issues with sound quality, ask the Chair to summarise what was said so that you get the full picture from the meeting.
- After the meeting, provide feedback to the chair about how it felt to attend remotely. Let them know where your experience might be improved. This may help future meetings for you or your colleagues.
- If using Microsoft Teams, you can also blur the background to help reduce any background disturbance. This is also useful if you are in the office and you are meeting with external colleagues.

Please note: When having a virtual meeting (VC or call) please be conscious of the environment that you are working in and consider whether it is appropriate to have those conversations particularly if sensitive or personal information is being shared. You should also be aware that some organisations

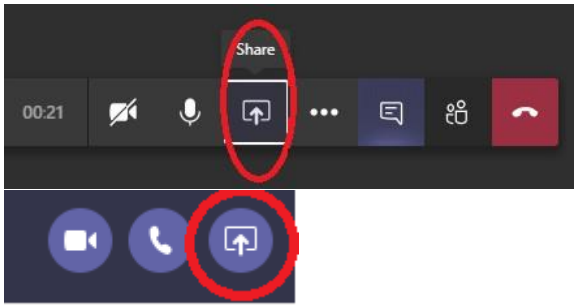
may have the ability to record their virtual meetings or conversations.

Sharing, Collaborating & Co-authoring

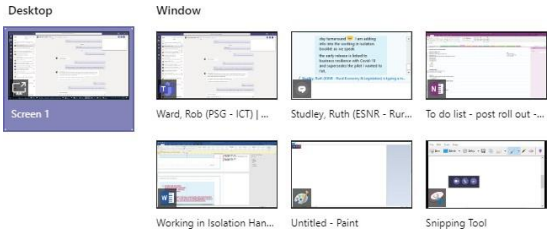
If you need to work with colleagues on a document, you may find that working remotely will provide the opportunity to try different ways of collaborating. For example, Microsoft Teams provides you with the ability to read, present and collaborate on the same version of a document in real time. This can be a very efficient way to co-author draft documents or receive agreement on a paper before leaving a meeting, rather than having to recirculate it afterwards.

Presenting/ Document sharing within Microsoft Teams

- If you are **within a call or VC** click on the 'share your screen' button on the task bar.

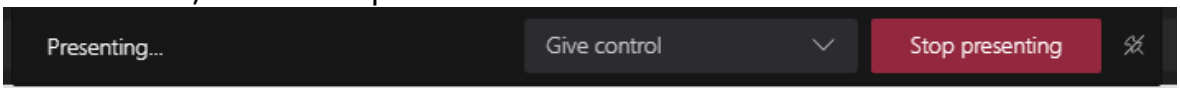


- If you are in a chat window, click on 'share your screen' in the top right corner of your Teams window.



- A window will open which contains all the open documents you have available. Select the one you wish to present.

- If you share a program, it will have a Now Presenting tab on your desktop. To stop sharing, click **Stop Presenting** on the bar at the top of your screen, or at the top of the conversation window.



- If another MTCBC colleague wishes to make changes to your document, they can request control, or you can give control which is in the grey bar as shown above.
- Colleagues outside of MTCBC are not able to make changes directly to a document shared via Present.

Please note: Individuals to whom you are presenting, can only see the

application you choose to share. They cannot see email notifications or pop up messages that may arrive whilst you are presenting.