Summary of Key Rules for Remote Working

1. During the COVID-19 crisis, remote working facilities are being extended to an increasing number of staff in CSO, as part of the Office's Business Continuity planning in response to the emergency situation. Remote working means conducting CSO work securely from a home environment, using a dedicated secure connection to the Office, called Reach.

2. The decision on who is enabled to work remotely and given relevant ICT resources is made by senior management, taking account of the CSO's priority statistical outputs and the nature of the work to be undertaken. It is hoped to facilitate most staff members who can use Reach.

3. Some tasks are not suitable for home working, either because they directly involve collecting confidential microdata; because they depend on working in an office infrastructure (e.g. posting out forms, scanning etc.); or because they depend on working in a team interacting in one location.

4. The exact tasks to be undertaken offsite must be agreed by the relevant Line Manager.

5. The CSO's remote access environment is being scaled up considerably for the duration of the COVID-19 crisis. The system has worked well with a small number of users but has not been tested or used actively with large numbers of users. In principle, the system should enable staff who are working remotely to carry out most of the tasks which they would normally do from their desktop. However, it probably won't be a perfect substitute for working in the office environment.

6. Your home working environment should be a private space. When working outside the office environment, you need to take extra care to protect statistical confidentiality:

    - You may not allow other members of your family or household to see any confidential information – e.g. statistical micro-data, statistical results you are preparing etc.
    - The locked screen rules which apply in the office should also be applied at home. Do not leave confidential information unattended.
    - You should not phone any survey respondents from your home (except for specific authorised data collection by household survey interviewers).
    - Any work phone calls you make should be in a private setting, without other members of your family or household present.

7. You must comply with all legal requirements which apply to your work in the CSO; and with all relevant CSO policies. These requirements include:

    - Compliance with Sections 32 and 33 (statistical use only and statistical confidentiality) of the **Statistics Act 1993**;
    - Compliance with the **GDPR** and **Data Protection Act 2018** (personal data should be processed securely and may only be used for the purpose for which it was obtained);

- Compliance with the CSO **ICT Acceptable Use Policy** (Office Notice 15/2015);
- Compliance with the CSO **Data Management Policy** (Office Notice 16/2019) – this policy sets out in detail the Do's and Don'ts of data management. It applies to remote working in the same way that it applies in the office.
- Specific attention is drawn to the **Security Best Practices and Policies** which are available from the CSO Lotus Notes homepage.

Links to the above-mentioned policies are being made available to all CSO remote access users.

8. Remote working gives you access to the same information you can process from your desktop in the CSO. It does this by means of a dedicated secure connection, which does not enable you to print or copy any information out of the CSO. You must not attempt to bypass these restrictions or copy any information outside of the CSO environment. In particular:

    - You must not copy any statistical dataset outside of the CSO, by email or any other means.
    - Copying or processing data outside of the CSO environment will be considered a serious breach of CSO policies and a breach of the Disciplinary Code.

9. Whether working in a CSO office location or from home, you are an Officer of Statistics appointed under the Statistics Act 1993. You have an obligation to keep the data given by our respondents confidential and to ensure the security of the CSO's data and ICT systems. You must not do anything which puts statistical confidentiality or information security at risk.

DO	DON'T
Agree your offsite tasks with your Line Managers.	Do not undertake offsite tasks outside of those agreed with your Line Managers.
Use the Softworks System to clock in/out. (Please note this is for record purposes only).	Do not log on – or attempt to log on – from any other location. Do not log on from public wi-fi provided by restaurants etc.
Follow the instructions given to you by CSO Technology for connecting remotely to your CSO account.	Do not carry out CSO work in a public space, such as cafes, trains etc.
Log on from home only.	Do not send CSO data or information to your home email or computer.
Keep your home working environment private.	Do not print (or try to print) CSO data or information at home.
Protect the passwords assigned to you.	Taking data outside the CSO ICT systems (e.g. sending it home, printing at home, etc.) will be considered a serious breach.
Protect any CSO ICT hardware (e.g. laptop, tablet, etc.) assigned to you.	