Coronavirus Pandemic

Information Security Measures – using Zoom and Other Web Conferencing for keeping in touch

Keeping in touch during the coronavirus pandemic is key for continuing to provide essential services and for teams to keep communicating. Web conferencing tools can play a key part in this.

Web Conferencing

Make sure you are familiar with Council guidelines on participating in Web Conferences including:

- Acceptable use and principles of web conferencing
- Tri-fold ready reckoner

Bear in mind that web conferencing tools are very powerful providing the ability to share files and desktop screens. Such actions should be undertaken with caution and in a way that does not put OFFICIAL-SENSITIVE information at risk.

Using Council Provided Equipment

The Council provides web conferencing tools on council owned equipment for staff to maintain communication.

Where you have been issued with Council owned equipment, such as a laptop or smartphone, this **must** be used for undertaking web conferences.

Web conferencing applications available include:

- Skype for Business;
- Teams;
- Zoom (for certain areas).

Using Personal Owned Computing Equipment

Where staff have no access to Council owned and managed equipment such as laptops, desktops or smartphones and there is an **urgent** or **ongoing need** during the pandemic to keep communication channels open it is generally accepted that personal owned devices can be used with Web Conferencing tools.

First Option – Use O365

Login to the Council's O365 to use Skype or Teams for collaboration. Refer to Questions 4 to 10 within the working securely guidelines for information on O365 and web conferencing from personal equipment.

Use must be done in such a way that:

- prevents the use of personal identifiable information;
- guarantees that unauthorised persons cannot gain access to the information shared within O365 i.e.
  - you must log out of O365 when not in use;
  - you must never save the password on a personal device;
  - if remaining logged into O365 due operational requirements, sharing of the device with others **must** cease and:

        - devices must be setup to auto lock when not in use and require a password / pin / phrase to be re-opened that is not known to any other party;
        - where biometrics is used to unlock the device any unauthorised parties setting must be removed while the device is being used for work communications.

Second Option – Webinar tools such as Zoom, GotoWebinar etc.

Login or connect to the Webinar ensuring use complies with Acceptable use and principles of web conferencing

This must be done in such a way that:

- prevents the use of personal identifiable information;
- guarantees that unauthorised persons cannot gain access to the information shared within the web conferencing tool i.e.
    - you **must** log out of web conferencing application when not in use;
    - passwords for connecting to the application must not be retained on the device;
    - if password being retained due operational requirements, sharing of the device with others **must** cease and:
        - devices must be setup to auto lock when not in use and require a password / pin / phrase to be re-opened that is not known to any other party;
        - where biometrics is used to unlock the device any unauthorised parties setting must be removed while the device is being used for work communications.

Official Council Records

Staff must ensure that any information shared within Web Conferencing is officially recorded within official council systems where there is a requirement for that information to be retained or audit logged.