

# working securely

## at WCC



## Confidentiality

Respect the confidentiality of personal or sensitive information that you have access to, on paper and electronic files. Handle it according to its risk and protective marking.

### Phone

Make sure the person is known, before giving personal or sensitive information. Be aware of who may be listening at either end.

### Email

Check the email address is correct whether internal or external. If information is marked as Protect or Restricted, you must encrypt if sending externally, be extra careful when using group names. Use Government secure mail, if applicable (e.g. Police, Local Authorities). Delete non-relevant history before sending. Consider electronic information sharing alternatives.

### Post

Always check the address is correct and contents are for the right recipient on the address. Double envelope if Protect with return address on outer envelope, use tracked mail if Restricted or secure courier for bulk items. Consider an encrypted electronic method as an alternative, e.g. encrypted USB or secure email.

### Fax

Only use if essential, always check the recipient is at hand to receive or check the number is correct with cover sheet first - don't use for Restricted.

### Printing/copying

Make sure you have the right printer set - test first if in doubt, collect print if not secure. Only print if essential. Must have protective marking on document, if Protect or Restricted.

### Storing paper

Lock personal and confidential documents and records in storage when away or not in use, especially overnight, keep a clear desk. If no longer required, dispose securely using confidential waste if Protect or Restricted, or send archive material to Records Management Service.



### Storing equipment

Lock away mobile equipment overnight. If no longer required return to ICT.

### Network and systems access

Use passwords that conform to the WCC password policy and lock your screen when away.

### Office access

Always show your security badge, challenge people if unknown, do not allow tailgaters to enter building. Always escort visitors and use public spaces or meeting rooms to meet, avoid a general office.

If you disregard these responsibilities as an employee, it may be regarded as misconduct and the Council's Disciplinary Procedure applies. A serious breach of any policy may be treated as gross misconduct and may lead to dismissal. For other staff engaged by the Council this may lead to termination of contract or agreement.

Should you need any help or further advice, please don't hesitate to get in touch with Information Security via the ICT Service Desk on:

**01926 (41)4141**

