CHILDREN'S SERVICES
Information Sharing Protocol

Issue Date:	**Issued By:**
8 January 2014 **Revised December 2015**	**John Macilwraith,** **CORPORATE DIRECTOR**

Summary of Instruction:

Children's Services receives and transmits a significant amount of Service User Identifiable data and confidential information. In order for us to operate efficiently we routinely exchange such information with others such as providers, health, and individuals. The Data Protection Act 1998 requires that we maintain the confidentiality of this information when transmitting it.

The definitions of user identifiable data are as follows:

- **Personal Identifiable Information** (PID) – (i.e. name, address, post code, data of birth, NHS number, or anything else which could identify an individual directly or indirectly such as specific drug treatments or rare diseases)
- **Sensitive Personal Data** - (such as racial or ethnic data, political opinions, religious beliefs, physical, health or mental condition, etc.)
- **Confidential Data** - i.e. information that it not normally in the public domain or readily available from another source i.e. financial data or employee information.

The procedure below should be used at all times to prevent any loss or breach of such information which could result in the Council facing a serious fine and/or the employee responsible facing disciplinary procedures. This method compliments the corporate Safe Haven Procedure For The Transfer of Service User Identifiable Information.

Information Sharing

- The data protection act is not a barrier to appropriate information sharing but it must be **necessary, proportionate, relevant, accurate, timely and secure**
- Information sharing is vital in safeguarding and promoting the welfare of children and young people. A key factor in many serious case reviews (nationally) has been a failure to record information, to share it, to understand its significance and then take appropriate action.

All staff need to be very clear that our duty to safeguard children overrides confidentiality. If it is safe to do so and you are not sure whether you can share information, please discuss this with your manager or ring the Safeguarding Hub (0333 240 1727). If the child appears to be suffering or likely to imminently suffer significant harm, please ring the Hub. You will be required to give the information over the telephone to enable a decision to be made about whether immediate action is required to ensure the child is safe. You will be asked to follow up your call in writing within 48 hours.

The LSCB Information sharing protocol can be found on the LSCB website (http://www.cumbrialscb.com/professionals/informationsharing.asp).

- Further guidance for practitioners and managers relating to Information Sharing can be accessed via the following links;

  Information sharing advice for safeguarding practitioners

Instructions for sending emails securely

The following provides instructions on the use of corporate email in the handling and sending of messages.

Where there is an alternative, personal information should not normally be transferred using the Microsoft Outlook Email system as there are some potential security issues and the potential for inadvertent disclosure. The sender should ensure that before transferring PID or sensitive data via email that there is no reasonable alternative route that provides a more secure method of moving sensitive data, such as the school portal for information for schools, or Objective Connect which is a secure file sharing system which can be set up for any recipient (Please contact the ICT service desk for assistance).

If there is a significant need to use email to exchange confidential information then it is essential that employees use a risk managed approach.

All Email (Internal and External)

All recipients should be carefully selected – avoiding the use of Distribution Lists wherever possible as these are often poorly maintained. Instead, there should be a conscious choice of recipients from the Email System. If they are necessary, distribution lists must be carefully managed and checked regularly. When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - e.g. “Dave” - the auto-complete function may bring up several “Dave’s”. Make sure you choose the right address before you click send. Double check the properties to confirm the role(s) of the chosen recipients.

1. Do not over use the cc facility. Data disclosure is on a ‘Need to know’ basis and users must be assured that they have sent PID to the minimum amount of people possible. A practice of minimum recipients should be adopted.

2. Be selective about who receives your e-mails, especially when using 'Reply to All'. Do all recipients need to see the reply?

3. Use BCC not CC if you do not have permission to disclose the addressees' email addresses.

4. Check all "thread" email messages before sending in case any previous messages in the "thread" contains confidential information.

5. Emails containing PID should be marked as CONFIDENTIAL in the subject header. The subject header should not include personal details. The body of the email should have a clear statement requiring the data to be deleted after use. All Cumbria County Council emails sent to external email accounts have a confidentiality disclaimer which appears at the bottom of the email.

6. All PID must be removed from mailboxes (sent items and deleted files folder) after transmission. If you need to keep a copy this should be saved in a secure folder.

7. Remember all emails are included in Freedom of Information and Subject Access Requests. You should always write emails on the basis that they could be seen by third parties in particular the individual being discussed.

Internal Mail

1. Internal emails within Cumbria County Council are considered to be secure. However PID information should not be included in the body of an email. If possible the data should be anonymous, use a commonly understood identifier or initials, instead of names. If PID information must be sent then this should be as an attachment. The body of the email should include the following statement – *This email has an attachment which contains personal information. If you are not the intended recipient you should not open the attachment. You should permanently delete the email and attachment and contact the sender.*

Secure Mail

1. In addition to internal emails there are other secure email addresses which are available such as cjsm or gsx. Few people in children's services have access to this type email. If you believe you need an account this will need to be authorised by the appropriate senior manager. Please contact the ICT service desk for assistance.

External Mail

1. All PID or sensitive data transferred by external email must be encrypted, using at least 256bit AES level of encryption. - Every PC/Laptop has the program 7Zip to provide this functionality. A password/key must be set on all encrypted data files with a minimum of 8 characters with a mix of numbers and letters. The password/key **MUST NOT** be transmitted in the same email but should be agreed with the recipient in advance of the transmission. Passwords should

not be open-ended – it should be a new password per transmission. You should save an unencrypted copy, in a secure folder, for future reference and delete the protected version once it has been sent successfully.

Please see appendix A for instructions on how to encrypt and password protect a file. Further assistance in the use of this is available from the ICT Service Desk.

2. All PID or sensitive data to be sent outside the organisation by email, which is not covered by an information sharing agreement, needs to be authorised and recorded by the Team. This should only be necessary in a small number of instances - (N.B. this process is currently being reviewed within the directorate and will be published once finalised)

Internet Email

1. Messages sent using commercial internet mail accounts (such as Gmail, yahoo or Hotmail) are particularly insecure and staff must not use them for council business

2. Do not sent PID to external email personal accounts such as xyz@hotmail.com or generic email addresses such as info@.....

Faxes

1. Confirm that it is urgent and absolutely necessary to send the information by fax. Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email.

2. Only fax confidential information such as a customer's identifiable information (name, address, date of birth) if any other means of identification (e.g. IAS number) which a third party cannot easily identify cannot be used.

3. Ensure that the fax contains the minimum necessary information to achieve its purpose. Make sure you only send the information that is required. For example, if a solicitor asks you to forward a statement, send only the statement specifically asked for, not all statements available on the file.

4. Ensure that highly sensitive information (mental health status, safeguarding) is not sent via fax.

5. Confirm to whom the fax should be sent by getting in touch with the recipient and inform them the fax is being sent, check fax number is correct and entered correctly.

6. Check if the fax was received by the "right" person.

7. Send a cover sheet first which

    - Is clearly marked "Confidential" as are all pages faxed
    - Has contact details for the sender (or use letter headed paper)

- Shows clearly for whom the message is intended.
- Contains the following message:

"The information in the fax is confidential. If you are not the above-named recipient of the fax, you are not authorised to read, keep, copy, alter or disclose the information of this fax as it is prohibited and may be unlawful. Please inform the sender – telephone number 0xxxxx-------- - about this error and return the fax to the above address immediately."

8. If a fax number will be used frequently, save it in the memory.

9. Monitor transmission and obtain a printed record of transmission.

10. All confidential faxes sent should be logged for future reference. (i.e. a team spread sheet with details of numbers, sender, receiver, date etc.).

Texts

1. Texting is generally an insecure method of information transfer.

2. No sensitive information should be sent via text.

Supporting Documents:

There is a dedicated area on Intouch relating to information security at Cumbria County Council - Information Security

ICO Guidance on the Data Protection Act

Cumbria County Council Records Retention and Disposal Records

Safe Haven Procedure For The Transfer of Service User identifiable Information

Information Security Acceptable Use Policy

Data Protection Act 1998

Date to be implemented:	**Any further enquiries to:**
With immediate effect	Shaun Smith, Business Systems and Information Manager

Implementation will be monitored through:

- Need to Know
- Monitoring Information Breaches and near misses

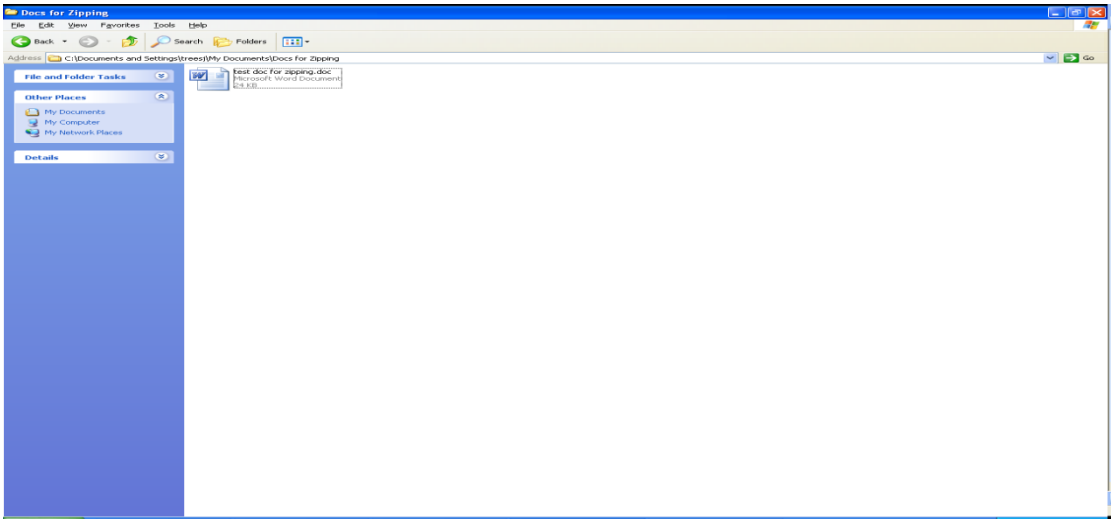
Appendix A

INSTRUCTIONS FOR ZIPPING / PASSWORD PROTECTING DOCUMENTS / FOLDERS AND SENDING VIA EMAIL (INTERNALLY OR EXTERNALLY).

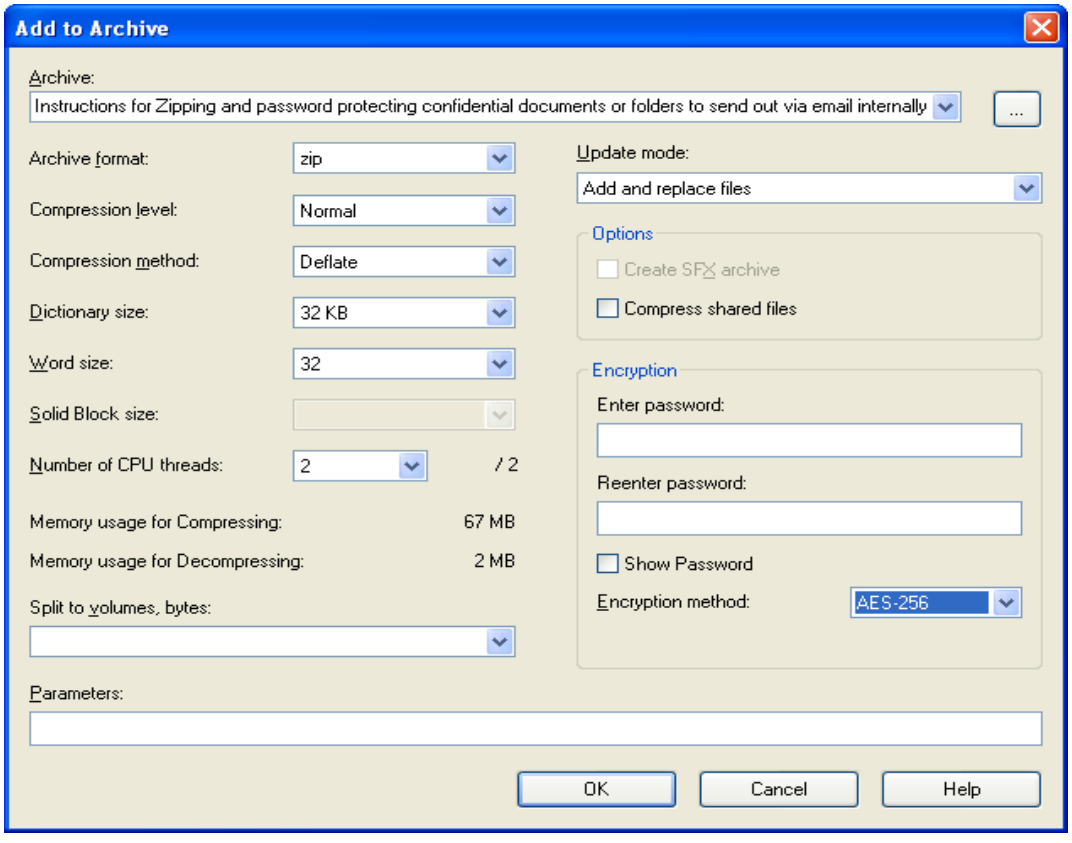
TO ZIP AND PROTECT A DOCUMENT (OR FOLDER)

1. Open the folder that has the document in it that needs zipping and emailing.

   Please note:-The document itself should not have an identifying name and should be renamed (or copied and the copy renamed) before starting the zip process.



2. When you have found the document you want to zip and password protect, right click on the document and select “7zip” and then “Add to Archive”
3. You will then get the screen below. In the Archive window rename the document so it has a non-specific name such as 20120910.zip – **DO NOT** USE specific names such as Julia Smith.doc or Julia.Smith.zip

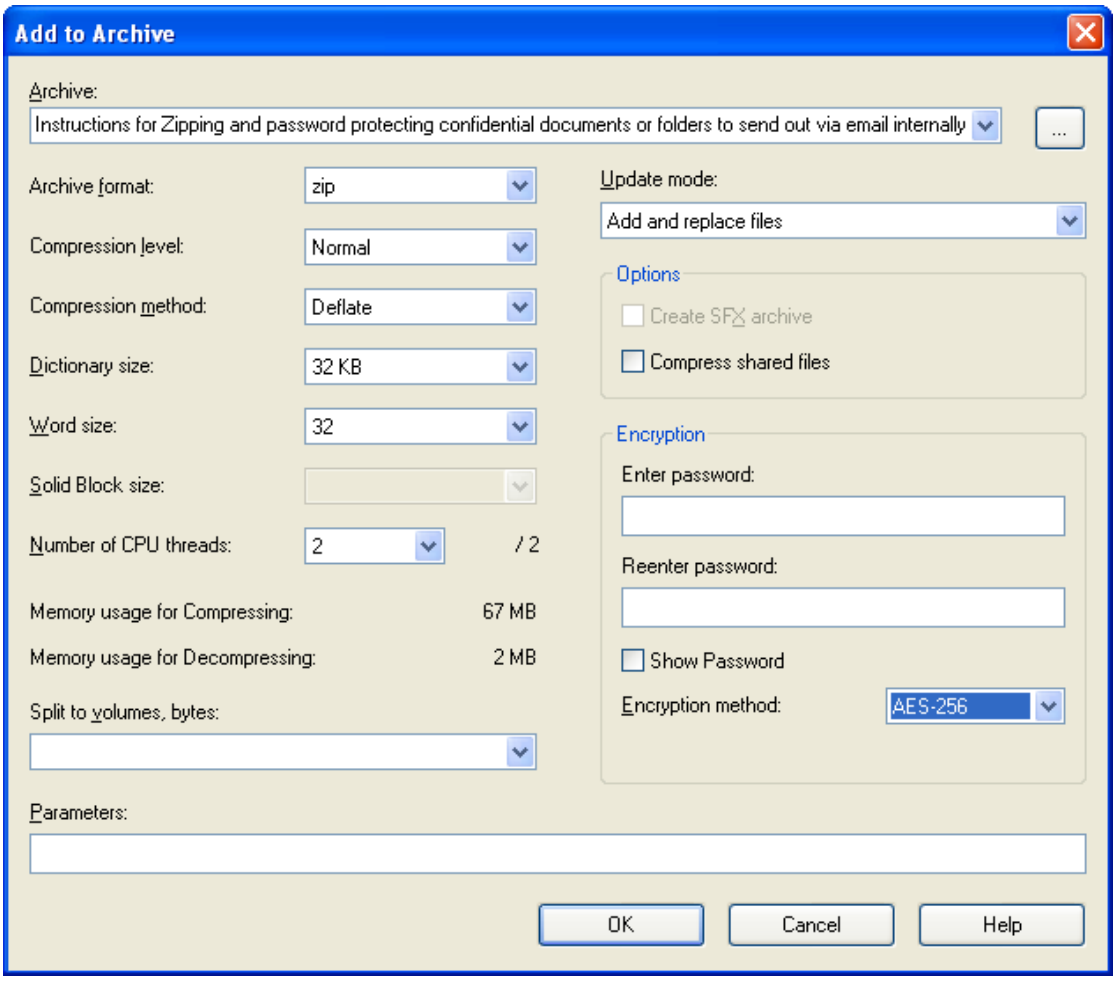


4. Using the drop down arrow make sure the **ARCHIVE FORMAT** field is set to zip

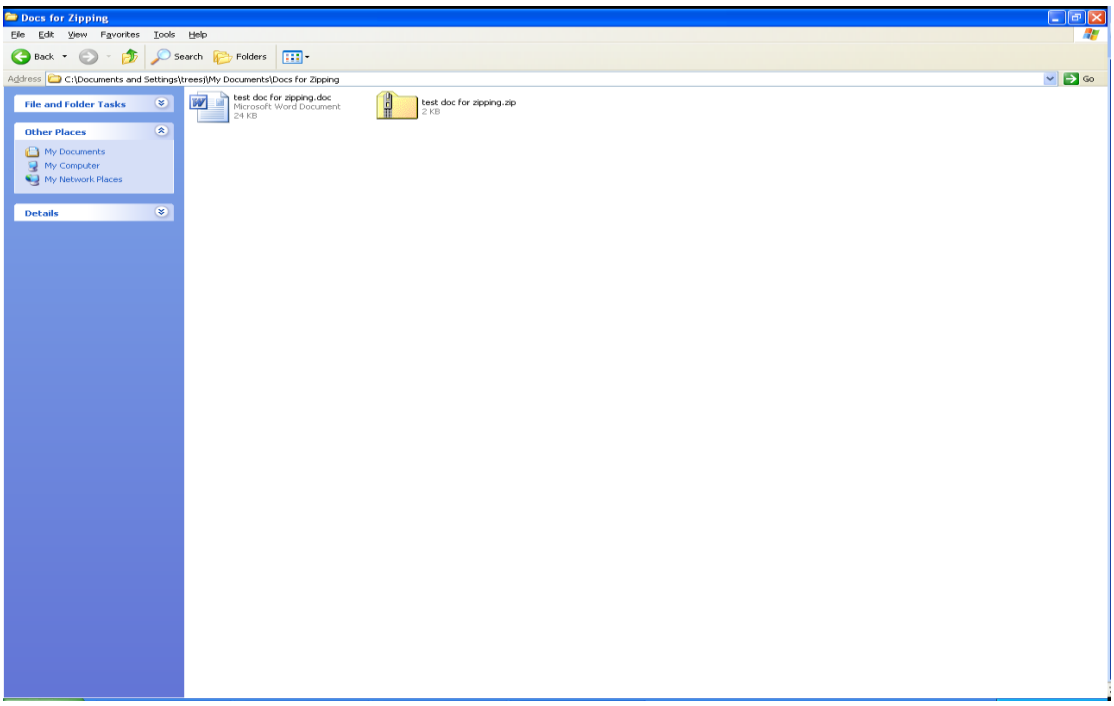
5. In the “Enter password” field – enter a strong password to password protect the document. Re-enter the same password again in to the “re-enter password” window.

   (An example of a good password is as follows :

   !2012JSOct02 (where the 4 numbers are the year, the initials of the person sending it and the Month and Day)

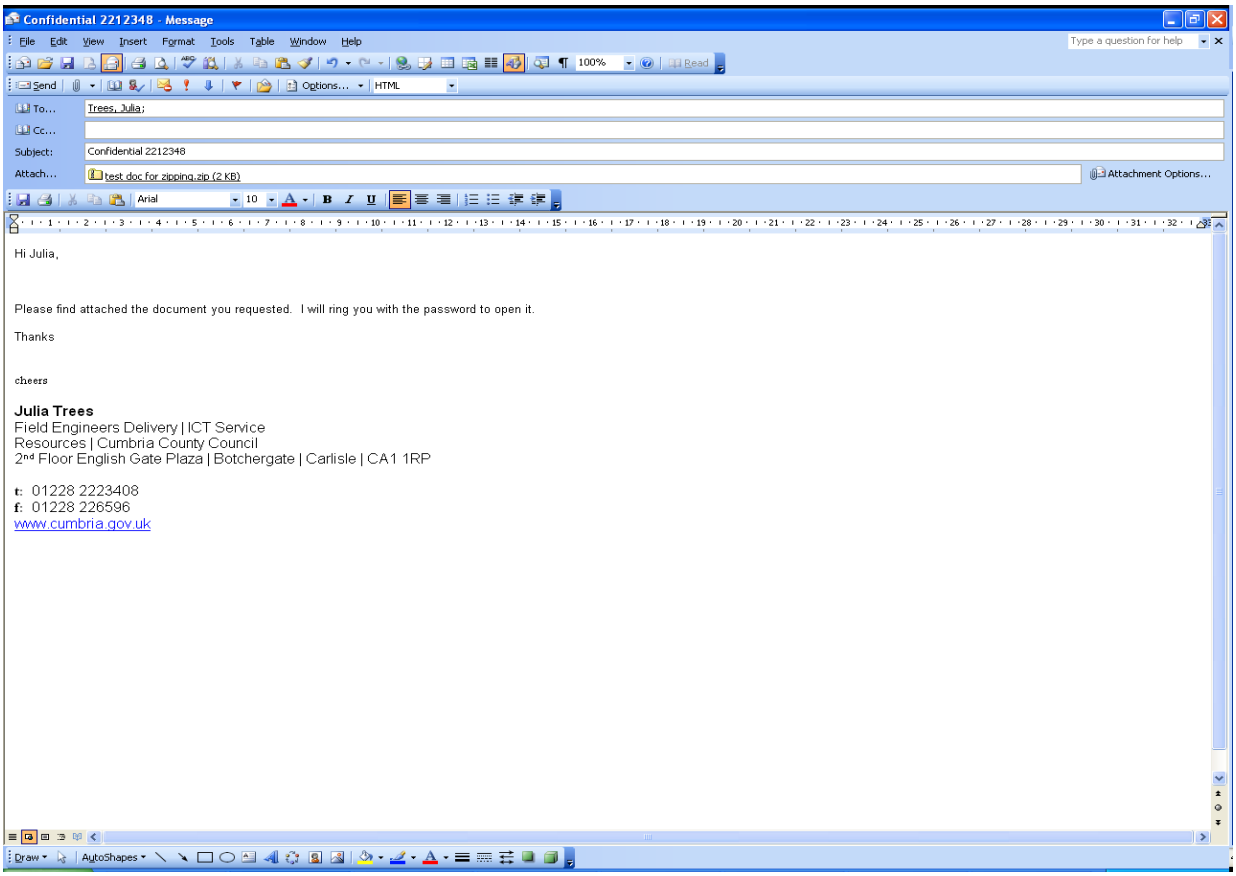


7. Under the ‘Encryption Field’ select the **AES-256** method.
8. Click on the OK button.
9. You will now see a copy of the document zipped in the folder as shown below.
10. To zip more than one document – create a new folder and move the files you wish to zip into it – then follow the instructions as above and select the multiple files



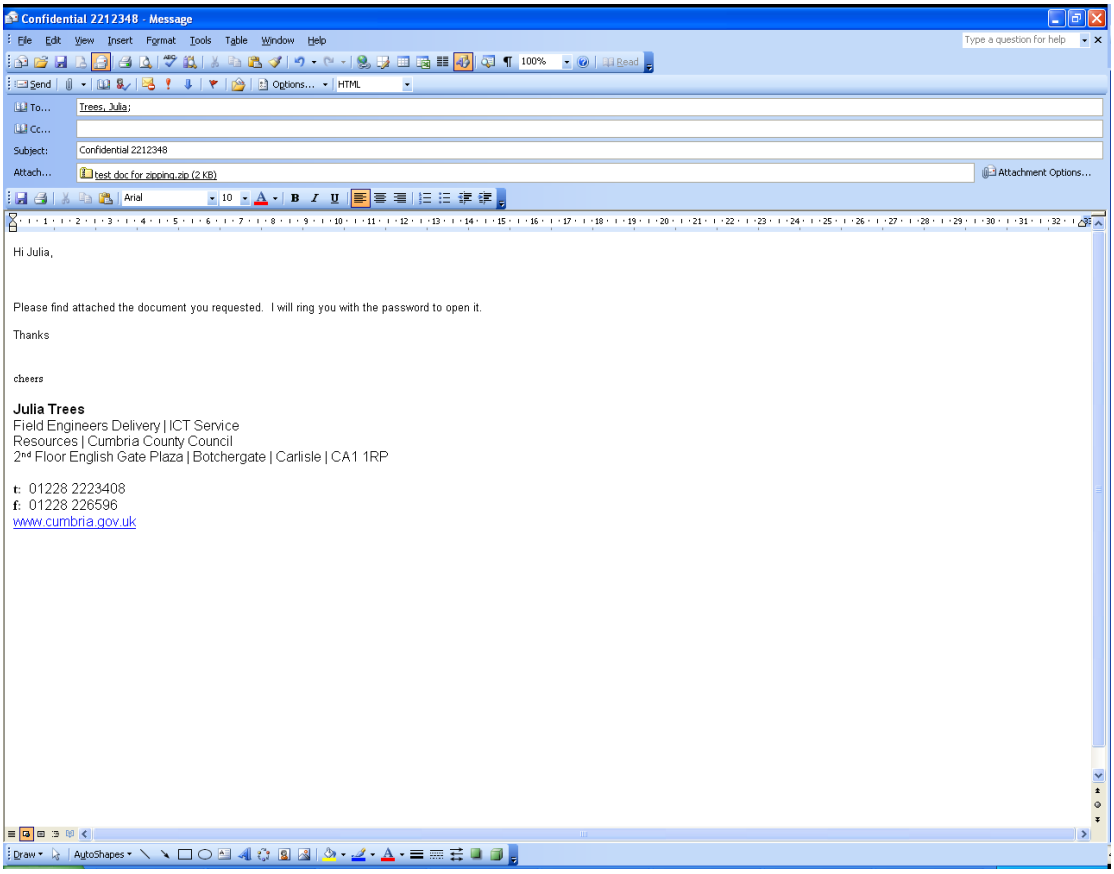
SEND AN EMAIL WITH THE SECURED DOCUMENT ATTACHED

1. Create a new email and enter the address of the recipient. If you wish to send to more than one recipient, – **DO NOT USE ADDRESS LISTS** - enter each address individually.
2. In the Subject field of the email please enter **CONFIDENTIAL**
3. **DO NOT** send the password in the email
4. Attach the zipped/encrypted file
5. The email you are about to send should look like this (see below):- with the zipped and password protected document attached.
6. **FINALLY – CHECK THE RECIPIENT LIST BEFORE SENDING**

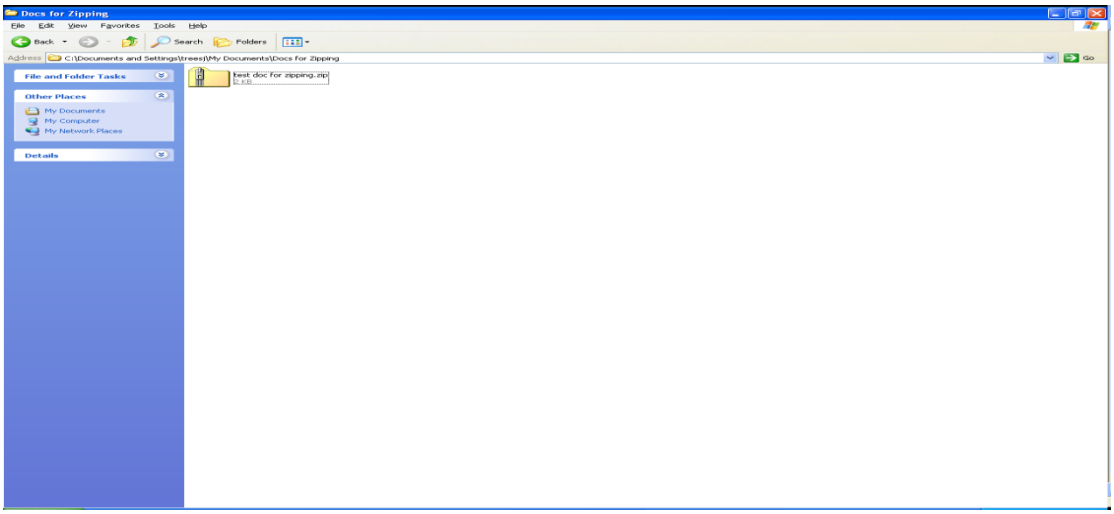


RECEIVING AND OPENING A ZIPPED AND PROTECTED FILE

1. Open the email containing the zipped.



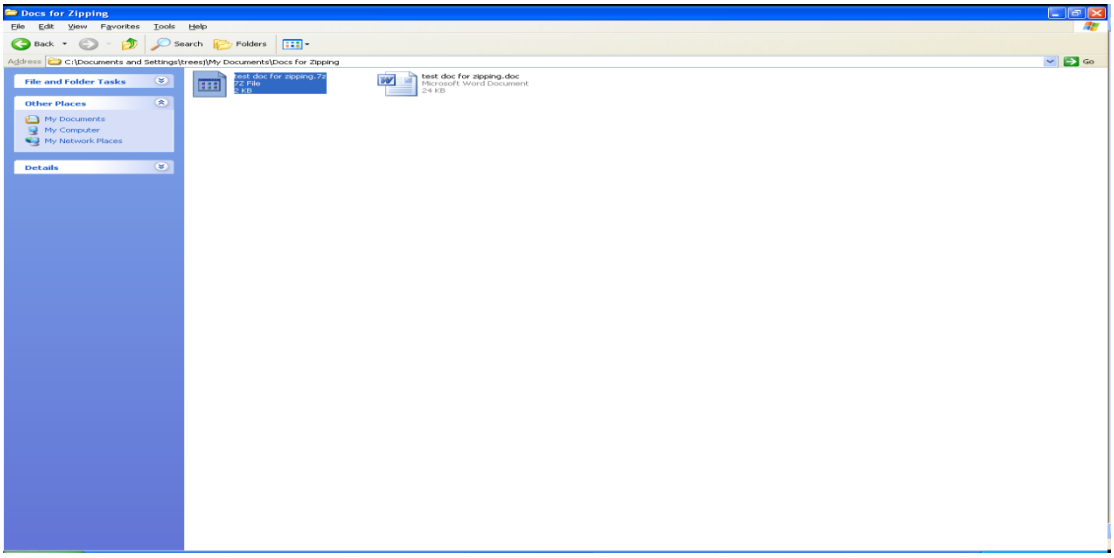
2. Right click on the attached document and select Save As and select a shared drive that you would normally save your documents to and save the document.
3. **DO NOT SAVE TO A USB STICK, REMOVABLE OR LOCAL DRIVE**



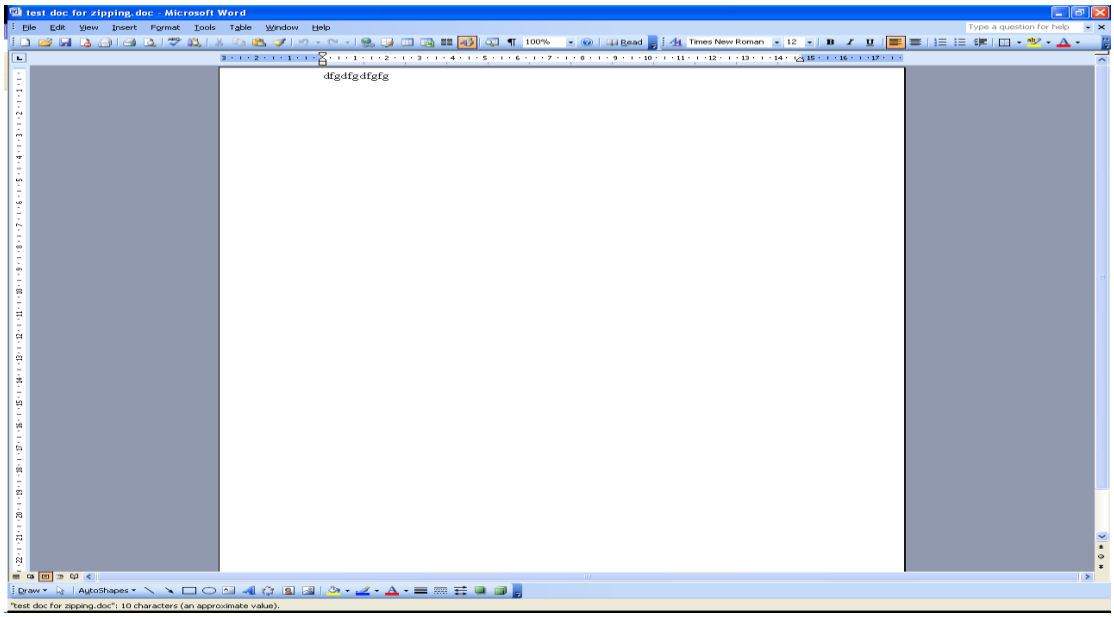
4. The sender of the email should ring you with the password to open the zipped document or folder.
5. If you have the password, Right Click on the zipped document that is in the folder share you have just saved it to.
6. Select “7zip” and then “Extract here”.

7. When prompted, enter the password to unprotect the document

8. The document will start to be extracted and will appear in the same folder but as a word document etc. as shown below.



9. You can now open it by double clicking on it and read the document as a normal unzipped document.



If you do not have 7zip installed on your PC or laptop then please place a call with the ICT Service Desk on 226000.