1. **Use of laptop**

As home working becomes part of the normal working practice of Organisation Name, you have been provided with a managed device, your laptop, to make that easier and safer. There are some precautions to take however to ensure the integrity of the data you handle.

1. **Confidentiality when video calling**

Wherever possible use a room that is not in use by other members of the house. If that is not a possibility use the headset that is provided when you need to have a meeting that may require discussing sensitive topics such as social care, financial or significant policy matters. Also ensure you setup a background so your home working environment (and anyone/thing in the vicinity) cannot be seen.

For further information about how to use remote working programmes such as MS Teams, Skype and Zoom and see the guidance here; Insert appropriate link

1. **Phishing**

Phishing is a type of cyberattack that involves someone tricking you into thinking that you are giving details such as passwords or account information. Such emails will tend to have identifying features such as an urgency for the information or threat if it is not supplied in time, a reward and, may not refer to you by name. A full list of the things to look out for can be found here: Insert appropriate link

Any suspicious emails must be sent to: Insert appropriate link

1. **Shoulder Surfing**

Unfortunately, it isn’t always possible to work in an isolated room, of course family members are trustworthy but the disclosure of another person’s personal data to them where there is no justifiable reason is a data breach and must be avoided. Lock your screen whenever you’re away from it by pressing the Windows key and L.

1. **Storage and Disposal of Paper Records**

You may still need to use physical records, if so, you should keep them out of sight when not in use and secure them at the end of the day in a place that is not in general use and if possible in a locked place. This is especially relevant for records that relate to safeguarding, special categories of personal data and sensitive business information. If you use a notebook for your work you should use initials where possible, avoid writing excessive information and use a notepad that is specifically for work not the general household notepad.

If you need to dispose of records and have a crosscut shredder that meets level 3 you can dispose of them at home. If you do not, then securely store the records until you are able to bring them back onsite and place them in a confidential waste bin or shredder.

If you are unsure about what your shredder can do please use look at the information on the website here <https://www.the-shredder-warehouse.com/security-level> If you are still in doubt wait to dispose of it onsite

1. **Using Laptops, Phones and Tokens**

The devices that you have should only be used for School/Council purposes and not for personal use except in exceptional circumstances. Further information about acceptable use can be found in the Acceptable Use Policy Insert appropriate link

When not in use the device should be shut down and secured, this may mean in an isolated room or if necessary, in a drawer or lockable cabinet. It must not be left on display or near an easy access point in your house.

1. **Sending Emails**

The most common cause of data breaches is sending emails to the wrong address, with the wrong attachments or not blind carbon copying (BCC) them when they should be. As a lot more communication is now going via email this risk is increased, so before sending any email remember the steps below:



1. **Sending Post**

If you need to send post you should insert appropriate policy here

1. **Do’s and Don’ts**

Some general pointers to remember:

 **Do:**

* + Keep your devices secure
	+ Ensure that the data used on the devices is secure at all times
	+ Report any suspicious emails
	+ Pause before you send emails to ensure they are correct
	+ Carry out your work in a safe location

 **Don’ts:**

* + Share your device
	+ Leave it unlocked when not in use
	+ Respond to emails requesting personal data or passwords without close inspection
	+ Use your device in a public location if possible
	+ Have a meeting discussing sensitive issues without using a headset
1. **Freedom of Information (Remove where not appropriate)**

Please note that the Freedom of Information Act (FOIA) entitles a requester to seek information held by organisation name in a recorded format (subject to any applicable exemptions).  As a result, it is worth remembering that almost any information that you hold/create could be captured within the scope of a FOIA request.  This can include information in any format (within reports, emails, drafts etc).  All Freedom of Information responses are drafted/reviewed (and exemptions applied where appropriate), before being disclosed. You should read the FOI policy if you are unsure about actions to take.

1. **Records Management**

When working from home paperwork should be avoided if at all possible. If completely necessary, ensure you have somewhere to store it - a lockable location is preferable but not 100% necessary.

Emails are not a storage location! If an email has any business value it should be saved elsewhere. Email is the envelope, not the letter.  There isn’t a specific retention period for emails, the information that they contain should be filed in the relevant location and the email deleted.

When sharing documents with other members of staff, send a link to a file/file location this will reduce the burden of emails.

1. **Who to Contact**

For IT issues with your devices report these via Insert appropriate link.

For data breaches follow the instructions Insert appropriate link to Data Breach Policy / Reporting Form

For any other data protection matters contact Insert appropriate link or your DPO i-west@bathnes.gov.uk