



Cyber Security & Data Protection

Policy

The Company has addressed the question of cyber security by drawing up a Cyber Essentials policy document which governs the day-to-day use of information systems in the place of work and in accordance with which this document has been formalised.

Security

The questions of cyber security and personal data protection affect many aspects of everyday activities undertaken by members of the team and must be taken extremely seriously. The Company has a General Data Protection Regulation ("GDPR") Transparency Notice for business contacts available to view and download on the Company website and an Employment GDPR Transparency Notice for employees, which is part of their Company Manual and which also is issued to job applicants.

Definitions

Folio	The Bluemay and Bluemay Weston mainframe system
Device	PC, MAC, desktop computer, laptop, tablet, smart phone or other computing device not here specified
Data Media	Memory stick, external hard drive, flash drive, USB stick, floppy disk, CD, DVD or other portable means of holding and using computer files

Accessing **Folio** and/or work desktop at work

- Access **Folio** from your allocated screen. You also may access any unused screen that is available at work. Remember to log off when you have finished your session or when you have to leave the screen unattended and to use a disinfectant to wipe over the mouse and keyboard after you have finished.
- If appropriate to your job, access your work PC desktop at your own desk.
- Ensure your allocated PC has up to date anti-virus definitions and that any operating system software updates have been installed. If in doubt, consult a Manager. Managers are responsible for keeping software up to date on unallocated PCs.

Third party data/programs

- Do not use third party or unknown **Data Media** and do not download files or programs or start or double click on executable files or programs without permission from a Manager or Director.
- When you have permission, where possible always scan **Data Media** with anti-virus and/or anti-malware software before opening

a folder or file. If you do not know how to scan a file or an email attachment, ask for help.

- When you have permission, where possible download any executable files or programs to a memory stick and scan the stick with authorised anti-virus software before opening the file or running the program.
- Do not leave **Data Media** in place unattended.
- Please use the proper **Data Media** ejection process. Failure to observe the ejection protocol could result in corrupted data.
- Check that webpages have a secure connection padlock symbol at the beginning of the address bar.
- Do not click on links on unsecure or unverified website pages.
- Stop work immediately and inform a Manager if you are redirected to an unexpected web page or if you notice anything unusual, different or strange about the web page you are using, including unexpected pop-up windows.
- Private browsing online using workplace computers is strictly forbidden without case-by-case specific authorisation from a Manager or Director
- Do not click on suspicious email attachments.
- Always be wary of email attachments and call a Manager or Director if you see anything suspicious in an email, including:
 - an incorrect sender email address,
 - lack of proper opening to the email message,
 - spelling or grammar errors in the email message or
 - an unexpected attachment or type of attachment.
 - a request or demand for urgent or immediate action
 - a request to click on an unusual or unexpected link within the email
 - If you do not know how to scan a file or an email attachment for viruses or malware, ask for help.

Accessing **Folio** and/or work desktop remotely (from off-site)

- Access **Folio** and/or your work desktop using only a known **Device**
- Where possible use VPN for secure access to **Folio** from a home PC.
- Only use a PC which is running reputable real time anti-virus and/or anti-malware software.
- Do not use third party or unknown **Data Media** and do not download or start executable files or programs without permission from a Manager or Director
- Ensure real time anti-virus and/or anti-malware software is running on the **Device** before attaching or inserting **Data Media** and before downloading executable files or programs.
- When you have permission, where possible download any executable files or programs to a memory stick and scan the stick with authorised anti-virus software before opening the file or running the program.
- Sign out of both **Folio** and VPN connection if you need to walk away from the connected **Device** unless you are in a secure environment and **always** sign out of your **Folio** profile and VPN connection after you have finished.

- Use TeamViewer on a known **Device** only to access your work desktop for **Folio** and/or your work files. Sign out of both **Folio** and TeamViewer connection if you need to walk away from the connected **Device** unless you are in a secure environment and **always** sign out of your **Folio** and TeamViewer profile after you have finished.
- Do not download Company documents to your local **Device** without permission from a Manager and regularly check such downloaded documents with a view to deletion where possible.

When using your own remote **Device**

- Ensure every **Device** has a password with auto-lock set
- Ensure all work-related files on the **Device** have a password or are restricted to your access profile only
- Delete any temporary files or files without a password before you finish your work session and remember also to delete the documents a second time from the Recycle Bin, Rubbish Bin or Recently Deleted section (as appropriate) of the **Device**
- Do not allow passwords to be stored or recorded on an unknown **Device**
- Ensure all passwords are kept on a secure document at work with access allowed to Managers. Managers will review these and require replacement of inadequate/poor-security passwords
- Do not use email apps or smartphones for work email addresses – use full browser log on with a laptop or desktop computer protected by real time anti-virus software.
- Ensure any work account connection is logged off after use

Email

- Currently the Company makes use of Gmail “alias” email addresses configured to send and receive messages as Company emails
- The Gmail sign on details must be kept on a register by the General Manager or Company Data Coordinator.
- Two step verification must be turned on for the Gmail address sign on. The verification telephone number must be an office telephone number which does **not** belong to the individual using that Gmail account and the back-up email address for office Gmail addresses must be that of a Director or of the Company Data Coordinator.
- Gmail accounts for Company email addresses must be accessed on a desktop or laptop computer running current real time anti-virus software. Mobile phones and home computers should not be used to access Company emails and Gmail accounts without express permission in writing from a Director.
- Personalised Company email addresses should not be used for placing supplier orders and any customer placing an order on a personal Company email address should be politely requested to use the standard Company email address.

The Directors, while retaining responsibility for Data Protection, have appointed an in-house Data Co-ordinator whose name will be posted on Company notice boards. The Data Co-ordinator will collaborate with Managers to collate, action and keep records of personal data requests as well as keeping a central record of account names and passwords for Company online accounts.

The **Folio** computer system governs the change of sign on password on a regular basis for each individual. Passwords should consist of a mix of letters and characters and not be easily guessable. Do not set passwords such as the user's date of birth or child's name, nor such simple codes as "123". It is the responsibility of those members of the team with access to online Company accounts to change their various access passwords regularly and to keep updated details using the appropriate form which will be held by their Manager.

Those members of the team whose job includes the processing of personal data should ensure that data is stored in a manner which is secure but readily retrievable if required for personal data request purposes.

Anyone discovering a lapse in or breach of data security – in other words, where unauthorised access is possible to private personal data – should report the matter immediately to the Data Co-ordinator or, if unavailable, a Manager or Director. This can be in person, by email to gdpr@bluemayweston.co.uk or by telephone.

Software

In addition to the **Folio** software system and any appropriate programs bundled as part of a computer package, standard software programs should be used on company PCs to ensure consistency across the Company and are as follows:

Operating System	MS Windows Mac OS
Word Processing (if Folio is not appropriate)	Microsoft Word
Spreadsheets	Microsoft Excel
Web Browsers	Mozilla Firefox Google Chrome Microsoft Internet Explorer Microsoft Edge Apple Safari
PDF viewers	Adobe Acrobat
Antivirus for all internet PCs	Authorised comprehensive Anti-virus protection system
Scanning (other than PhotoFile)	Bundled scanner software
Back up	Windows Back Up Apple Time Machine Macrium Reflect

All PCs will be configured to auto-install software updates, either directly from the internet or via another PC on the network with an internet connection. Office staff will be given training on checking to ensure that software is updated regularly on the PCs used by them. Other PCs (generally using just an operating system with **Folio** and Adobe Acrobat) will be subject to regular software update checks.

Permission must be obtained from a Director or Manager before any other programs or executable files are downloaded from the internet or loaded from **Data Media** or a portable **Device** or transferred from another computer onto a Company computer.

Only approved suppliers or their authorised representatives with prior Directorial permission are allowed physical or remote access to Company computers. Personal or other third party **Data Media** should not be used with Company computer equipment without prior approval by a Director.

Email & Internet

Emails are items of mail, just the same as letters, and the person operating the computer on which emails are received is merely the equivalent of a letter opener. It is vital that time is not wasted reading irrelevant or unnecessary emails. Emails with attachments are like parcels and, like parcels, attachments must be opened only with care. The email equivalent of a mail bomb is a virus-carrying attachment. It is therefore a condition of employment that only authorised and trained staff use the email facilities, in line with this policy.

The internet represents a source of almost limitless information, but also can be a tremendous waste of time and money. Surfing the net for anything other than Company requirements is at best a misuse of Company resources. It is therefore a condition of employment that only authorised and trained staff use the internet facilities, in line with this policy.

Use of the internet should be for specific business purposes only, such as marketing research or parcel tracing, and should be carried out only by an email operator whenever possible. Use of the internet for personal matters is not allowed without specific permission of a Director in each case.

The person(s) authorised as the email operator(s) will

- ensure that regular checks for incoming emails are made throughout the working day (eg every two hours or as otherwise specified)
- that incoming emails are printed, distributed and, if appropriate, scanned to PhotoFile
- type, get approval for and send outgoing emails
- check every week that the virus protection software on the PC being used for email and internet connection is enabled and up to date

Members of staff with “named” email addresses, eg “bill@bluemayweston.co.uk” (rather than generic email addresses such as sales@bluemayweston.co.uk), must ensure that:

- Customers are encouraged to send order-related emails to the normal “sales” email address and not to the personalised address
- “Out of office” auto-generated messages are in place for planned absences from work, to inform those sending emails that the recipient is absent
- At least one colleague (of appropriate seniority) has access to the named email address in case of unexpected absences
- Company email addresses are not used for personal emails

Extreme care should be taken over any emails with attachments, or emails which request immediate opening via a pop-up box. If there is any doubt as to the origin, authenticity or safety of the email it should not be opened but left unopened for a Manager or Director to deal with. Extreme care must be taken not to surf untrustworthy websites, nor to click on email links or pop-up box links.

Email attachments should not be opened unless

- the source is trustworthy
- the message is expected

- the file type can be seen and recognized as conventional, and
- the attachment has been scanned by antivirus software.

The email operator should not waste time reading in full every email and attachment, nor should they reply to any incoming emails before that email is viewed and considered. Any incoming “spam” emails should be marked as junk or spam.

Emails should be removed from the “Deleted” folder on a weekly basis.

Authorised email operators

Any Director

Any Manager

Any member of staff authorized in writing by a Manager