Title:	IT and Digital Policy
Code:	WBITADP-01
Published:	November 2025
Review date:	June 2026
Approved by:	Senior Management Team
Policy owner:	Group Head of Estates

WaterBear is a College of Falmouth University, and as such its students are students of Falmouth University, studying at WaterBear. All WaterBear policies and procedures have been tailored to best suit the specific requirements of the College, its students and staff. In some instances, Falmouth policies and procedures may be deferred to for additional guidance, or where Falmouth policy has been deemed to cover both the requirements of the University's operations and those of its academic partners.

1. Policy Statement and Overview

1.1. The purpose of the WaterBear IT and Digital Policy is to establish acceptable practices and guidance regarding the use of WaterBear Information Resources to protect the security, confidentiality, integrity and availability of information created, collected, accessed and maintained through the use of Information Technology (IT).

1.2. This policy is in conjunction with policy WBDPCM-01 WaterBear Data Protection (compliance management) policy.

1.3. If there are any questions or uncertainties about anything contained within this policy, Users should contact IT Support for assistance and clarification.

1.4. This policy supersedes and replaces any previous ICT Information Security and Acceptable Use Policy as well as any separate Bring Your Own Device, Password and Remote Working Policies that may have existed prior to the publishing of this policy document.

1.5. This policy applies to any individual, entity, or process that interacts with any WaterBear Information Resource.

2. Policy Definitions

2.1. **Information Resource:** Any data or application or software held on any system. In the context of this policy this normally refers to Information Resources belonging to, or managed by, WaterBear.

2.2. **Information Technology (IT):** The physical devices and infrastructure used to store, access and share Information Resources, e.g. laptops, phones, networks.

2.3. **User:** Any person, entity, or process that interacts with any WaterBear Information Resource.

2.4. **Internal Information:** Any data generated from within WaterBear.

2.5. **Confidential Information:** Any data shared with a limited number of people for a specific purpose. The data may be confidential to all WaterBear Users, to a group or team, or to as few as two people.

2.6. **IT Management:** In this policy, this refers to Trident, who provide fully managed technology services to WaterBear.

2.7. **WaterBear Network:** Any secure Local Area Network provided at any WaterBear site. Currently, this only applies to the Brighton campus.

3. IT Support

3.1. The IT Support service for WaterBear Users is provided by trusted WaterBear technology partner, Trident. Users can contact the Trident helpdesk for advice or guidance on anything within this document via the following methods:

- Web: https://support.tridentgroup.co.uk/
- Telephone: +44 1273 662777 (select option 2 for Technical Support)

Please note that for any security-related issue (e.g. if a User suspects their account may have been compromised) you should telephone in the first instance to ensure as rapid a response as possible.

4. Acceptable Use

4.1. **Acceptable Use:**

- **Users** are responsible for complying with WaterBear policies when using WaterBear **Information Resources**. If requirements or responsibilities are unclear, please seek assistance from the Policy Owner.
- **Users** must promptly report harmful events or policy violations involving WaterBear physical assets or **Information Resources** to their line manager. Events include, but are not limited to, the following:
    - <u>Technology incident:</u> any potentially harmful event that may cause a failure, interruption, or loss in availability to WaterBear **Information Resources**.
    - <u>Data incident:</u> any potential loss, theft, or compromise of WaterBear information.
    - <u>Unauthorised access incident:</u> any potential unauthorised access to a WaterBear **Information Resource**.
    - <u>Policy violation:</u> any potential violation to this policy.
- Users should not purposely engage in activity that may degrade the performance of WaterBear Information Resources, deprive authorised WaterBear Users access to a WaterBear Information Resource, or circumvent WaterBear computer security measures.
- All inventions, intellectual property, and proprietary information, including reports, images, blueprints, software codes, computer programs, data, writings, and technical information, developed on WaterBear time and/or using WaterBear **Information Resources** are the property of WaterBear.

- Use of encryption should be managed in a manner that allows designated WaterBear **Users** to promptly access all data.
- WaterBear **Information Resources** are provided to facilitate the organisational business and should not be used for personal or financial gain.
- **Users** are expected to cooperate with incident investigations.
- **Users** are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using WaterBear **Information Resources**.
- **Users** should not intentionally access, create, store or transmit material which WaterBear may deem to be offensive, indecent, or obscene.

4.2. **Accessing Our Systems:**

- Access to information is based on a “need to know” basis. This means a **User** will only have access to the information that’s required for their job function.
- **Users** must not attempt to access any WaterBear data, programs or services for which they do not have authorisation or explicit consent.
- All remote access connections made to internal WaterBear networks and/or environments must be made through methods and tools that have been approved and provided by WaterBear methods and tools only.
- **Users** should not divulge any access information to anyone not specifically authorised to receive such information, including the IT Support team at Trident.
- **Users** must not share their personal authentication information, including:
    - Account passwords.
    - Personal Identification Numbers (PINs).
    - Security Tokens (i.e. Smartcard).
    - Multi-factor authentication information.
    - Access cards and/or keys.
    - Digital certificates.
    - Similar information or devices used for identification and authentication purposes.
- Access fobs and/or keys that are no longer required must be returned.
- Lost or stolen access cards, security tokens, and/or keys must be reported as soon as possible.
- A service charge may be applied for access cards, security tokens, and/or keys that are lost, stolen, or are not returned.
- **Users** should log off from applications or network services when they are no longer needed.
- **Users** should log off or lock their workstations and laptops when their workspace is unattended, even if only for a few minutes.

4.3. **Data Security:**

- **Users** must only use approved encrypted communication methods whenever sending **Confidential Information** over public computer networks (Internet). Outlook mail encryption is approved. If **Users** need advice about encryption, or are uncertain, they should contact IT Support.

- When WaterBear Users need to manage the sharing, storing or transferring of Confidential Information or Internal Information they should only use authorised cloud applications. These include:
    - Microsoft 365 Tools (e.g. OneDrive, SharePoint or Teams)
    - Canvas (VLE)
    - Eventmap Timetabler / Booker
    - Hubspot
    - WhatsApp may be used for conversations but should not be used for sharing files containing Confidential Information.

- Where external third parties require WaterBear Users to share data on their own preferred applications, Users may not share Confidential Information. Users should be aware of the risks when they use these applications and be sensitive about what they share. External applications sit outside of our control and therefore security, distribution and confidentiality cannot be assured. Examples of such third-party data-sharing tools that should be used with caution and only when externally requested include (but are not limited to):
    - DropBox
    - BOX
    - WeTransfer
    - Google Docs

- If users want to manage the sharing, storing or transferring of Confidential or Internal Information using applications not in the authorised list they must contact IT Support prior to use so the request can be reviewed and assessed, and if a suitable business case can be established, an appropriate exception may be granted if necessary.

- Information must be appropriately shared, handled, transferred, saved, and destroyed, based on the information sensitivity.

- All electronic media containing **Confidential Information** must be securely disposed of. Please contact IT Support for guidance of assistance where needed.

4.4. **Email and Electronic Communication:**

- Automatic forwarding of emails to recipients outside the WaterBear internal systems is prohibited.
- Spoofing and similar deception is strictly prohibited. This means that Users must never send emails or electronic communications which pretend to come from someone else or from another organisation.

- Users are responsible for the accounts assigned to them and for the actions taken with their accounts.
- Users must not share their account details (e.g. Username and password) for any WaterBear system or service with any other parties.
- Users must not grant access to their own account(s) without prior authorisation from IT Support.
- Staff should not use personal email accounts to send or receive WaterBear Confidential Information.
- Any personal use of WaterBear email service should not:
  - Involve solicitation;
  - Have the potential to harm the reputation of WaterBear;
  - Forward chain emails;
  - Contain or promote anti-social or unethical behaviour;
  - Violate local or international laws or regulations;
  - Result in unauthorised disclosure of WaterBear Confidential Information;
  - Or otherwise violate any other WaterBear policies.
- Users should only send Confidential Information using approved secure electronic messaging solutions. Users should consult IT Support if unsure of when or how to achieve secure messaging. For the avoidance of doubt, the following types of data are expressly required to be sent using a secure solution:
  - Bank details of any person or organisation
  - Personal contact details of any individual
- Users should use caution when responding to, clicking on links within, or opening attachments included in emails, Teams chat messages, and any means of electronic communication. Particular caution should be exercised when they originate from outside of WaterBear.
- Users should use caution when disclosing Confidential or Internal Information in Out of Office or other automated responses, such as employment information, internal telephone numbers, location information or other potentially sensitive or personal data.

4.5. **Hardware and Software:**

- When working on the WaterBear Brighton campus or Sheffield campus, or any other site with a dedicated WaterBear Local Area Network:
  - Only equipment (laptops, phones, tablets etc.) that have been issued by WaterBear may be connected to WaterBear internal networks.
  - Any equipment that has not been issued by WaterBear (such as personal mobile phones or visitors' laptops) should only be connected to relevant 'Guest' or 'Visitor' network(s).
- All software installed on WaterBear equipment must be approved by IT Management and installed by WaterBear IT Support.

- All WaterBear assets taken off-site should be physically secured at all times, e.g. not left in plain sight inside vehicles, kept in secure storage when not in use, not left unattended when in open or public spaces.
- Users should not allow family members or any individuals that are not WaterBear staff, students or contractors to use WaterBear equipment.

4.6. **Internet:**

- The internet must not be used to communicate WaterBear Confidential or Internal Information, unless the confidentiality and integrity of the information is ensured and the identity of the recipient(s) is established.
- Use of the Internet with WaterBear networking or computing resources must only be used for business-related activities. Unapproved activities include, but are not limited to:
  - Recreational games
  - Accessing or distributing pornographic or sexually explicit materials unless expressly required for the work of WaterBear.
  - Attempting to make or making unauthorised entry to any network or computer accessible from the Internet
  - Otherwise violating any other WaterBear policies
- Moderate use of the Internet for personal activities is allowed during working hours, so long as the usage does not cause any negative impact to the business (e.g. cause the Internet service to slow down for other Users etc.). See the 'Personal Use' section further down for more on this.
- **Users** may work with their WaterBear laptop from any location, but if the Internet is accessed from outside the WaterBear network they must adhere to all of the same policies that apply to use from within WaterBear facilities.
- **Users** are responsible for protecting WaterBear equipment from damage. Caution must be used when eating or drinking near any IT equipment such as workstations, laptops or mobile devices.

4.7. **Privacy:**

- Information created, sent, received, or stored on WaterBear Information Resources is not private and may be accessed by WaterBear IT employees at any time, under the direction of WaterBear management and/or People Team, without knowledge of the User or resource owner.
- WaterBear may log, review, and otherwise use any information stored on or passing through its Information Resource systems.
- Systems Administrations, WaterBear IT Support, and other authorised WaterBear Users may have privileges that extend beyond those granted to standard Users. Users with extended privileges should not access files and/or other information that is not specifically required to carry out a valid employment-related or support-related task. If there is any doubt, please check with WaterBear management or IT Support.

4.8. **Removable Media:**

- **Removable media** is any type of storage device that can be removed from a computer whilst the system is running, e.g. USB memory sticks, external hard drives, removable disks.
- The use of **removable media** for storage of WaterBear information must be supported by
- **Personally owned removable media** use is not permitted for storage of WaterBear information.
- Users are not permitted to contact **removable media** from an unknown origin without prior approval from WaterBear IT Support.
- Confidential and internal WaterBear information should not be stored on **removable media** without the use of encryption. If Users need assistance in ensuring removable media is suitably encrypted, they should contact IT Support.
- All **removable media** must be stored in a safe and secure environment when not in use.
- The loss or theft of **removable media** that may have contained any WaterBear information must be reported to WaterBear IT Support as soon as the loss is discovered.

4.9. **Personal Use**

- As a convenience to WaterBear Users, incidental personal use of Information Resources is permitted. The following restrictions apply:
  - Incidental personal use of electronic communications, Internet access, printers, copiers, and so on, is restricted to WaterBear approved Users; it does not extend to family members or other acquaintances.
  - Incidental use should not result in direct costs to WaterBear.
  - Incidental use should not interfere with the normal performance of a user's work duties.
  - No files or documents may be sent or received that may cause legal action against, or embarrassment to, WaterBear or its staff, students or contractors.
- Storage of personal email messages, voice messages, files and documents within WaterBear Information Resources must be minimal.
- All information located on WaterBear Information Resources are owned by WaterBear and are subject to the same terms as detailed in section 10 Privacy.

5. Passwords

5.1. Password security is fundamental to the protection of WaterBear devices, systems, applications, and information. This policy describes WaterBear requirements as well as additional guidelines to assist Users in choosing a secure password. With certain credentials, the WaterBear password requirements are enforced, however in instances where this is not the case, the following policy guidelines must be adhered to.

5.2. All passwords to WaterBear systems and devices should have the following characteristics:

- Be at least twelve (12) characters in length.
- Must contain at least three of the following four types of characters:
    - Upper case letter
    - Lower case letter
    - Number
    - Special characters (e.g. !$%@&=)
- Passwords must not be posted on or under a computer or in any other physically accessible location.
- Passwords are not to be re-used (a history of at least six passwords will be enforced).
- Passwords cannot contain User account information (e.g. your name, names of relatives, your Username etc.)
- Passwords must not be shared with anyone and shall be considered as sensitive WaterBear information.
- Passwords shall not be written down or communicated via email as these methods are not secure.
- If passwords must be communicated by email, the email shall be encrypted. If Users are unsure how to send encrypted email or need help with securely sharing a password with someone, they should contact IT Support for assistance.
- Passwords used to access WaterBear resources shall not be re-used for personal services outside the organisation.
- New Users will be allocated a unique and secure password which will require changing upon the first login.

5.3. **Password creation guidelines.** When choosing a password, the following hints can help to ensure it is a secure password:

- Use three random words, with one or more numbers and/or symbols if you want, but do not use personal information.
- Do not include any personal information (DOB, name, relative or pet names, hobbies).
- Do not use single words that can be found in the dictionary (which can be cracked using a 'Dictionary' attack – where every word in the dictionary is tested).
- Do not use common passwords (e.g. 'Password1234' would suffice for the policy requirements but is NOT a secure password).
- Do not make the password TOO complicated. You should be able to remember it without having to resort to writing it down.
- Do not use the same password for different accounts.
- Do not use the same password for WaterBear accounts that you use for personal ones.

- Several Password Management applications exist that allow you to have many different secure passwords for accounts but only require you to remember the one that will give you access to the Password Management service or vault. If you would like advice about using a password manager, Users should contact IT Support for further guidance.
- Examples that would meet the requirements would include (these examples would all take longer than one hundred years to crack using current techniques):
    - 27SpeakerPlantWindow£
    - Bottle92SofaRain
    - !OrangeRoofCloud85

5.4. **Changing your password.** If at any point Users suspect that someone may know their password or, more importantly, that an account may have been compromised, Users must contact IT Support as a matter of urgency (telephone recommended) to report the incident. Steps can then be taken to secure the account, investigate any potential use of the compromised account details and remediate as necessary. Fast reporting of these types of incidents is crucial to keeping WaterBear data and services secure.

6. Mobile Devices

6.1. **Requirements:**

- This policy applies to all mobile devices that have access to WaterBear data, including file and email data. This applies to both company-owned and personally owned mobile devices such as smart phones and tablets.
- Mobile devices must be password or passcode protected. Device locking mechanisms such as biometric (fingerprint or FaceID), password or PIN, must be enabled to prevent unauthorised access to any organisational data or services that exist on the device.
- Device passwords must comply with the WaterBear password policy.
- The latest operating system and security updates/patches should always be installed, no later than 14 days after release.
- Users should be aware of the security risks when using public wireless networks to access company data and avoid accessing WaterBear information resources while connected to unsecure public networks where possible.
- Unsupported applications should not be used to access WaterBear information resources.
- Only approved applications should be used to access WaterBear information resources. Technical controls to restrict access to only approved applications may be put in place to enforce this. Users should consult IT Support for further advice with regards to approved applications if needed, or if a need to use an application, which is not listed as approved, arises.
- Users should take care when accessing company data to reduce the risk of potentially confidential data being overlooked by unauthorised people (e.g. over the shoulder reading of screens etc.).

- Any devices that have been ‘rooted’ or ‘jailbroken’ must not be used to access company data.

7. Home and Remote working

7.1. A home or remote worker is simply anyone who is working in a location where they are not connected to a WaterBear Local Area Network. Currently this means anyone not working on the WaterBear Brighton campus or Sheffield campus.

7.2. **Requirements:**

- Always adhere to the Password Policy (see previous ‘Password Policy’ section of this document).
- Do not leave any confidential information accessible in home or remote workspaces.
- If Users have been issued with a WaterBear laptop or other device, no one else should have access to it.
- There must NOT be attempts to disable, or over-ride company-developed security software (e.g. anti-virus software) or restrictions at any time.
- No unlicensed or not legally licensed software should be downloaded or installed on company devices.
- Users should comply with any legal requirements when it comes to computer usage and data protection.
- All company-related data should be saved, and worked on, directly from within Microsoft SharePoint, Teams or OneDrive.
- The User’s home router must incorporate firewall capabilities (most ISP supplied ones do). If Users are unsure, they should contact IT Support to check.
- The default password that the router was supplied with must be changed to a password that conforms with WaterBear’s Password Policy.
- The User’s home router/firewall should NOT allow internal services to be publicly accessible from the Internet unless there is a stated and documented business case for this.
- The User’s home router/firewall must be configured to block services from being advertised to the Internet by default (most ISP supplied solutions do this by default, but again, Users are advised to contact IT Support if they are unsure or concerned).
- The User’s home router/firewall’s administration console must NOT be publicly accessible over the Internet, unless restricted to nominated specific trusted public IP addresses only (and these should be documented to ensure that access is valid and reasonable). If Users are unsure, they should seek advice from IT Support.
- Any critical or high-risk updates made available for the User’s home router must be installed no more than fourteen days following their release.

- If Users have any questions, concerns or need further guidance when working remotely, they should contact IT Support.

8. Bring Your Own Device

8.1. WaterBear allows Users to use their own devices (e.g. smartphone, tablet, laptop) to access Company data and information whether at home or in the workplace. This section sets out the terms relating to the use of personal devices for accessing Company data.

8.2. **Requirements.** The use of personal devices is subject to these requirements:

- The device must have virus protection installed. This will be the User's responsibility – it must be active and always kept up to date.
- Company information may only be accessed on the personal device using the following applications:
  - Microsoft Suite
  - Canvas (VLE)
  - Event map – Timetabler /Booker
  - Payhawk payment system
  - Paxton key access app
  - CCTV and Alarm apps for Estates and Venue's staff
  - Any applications via the web browser (Edge, Chrome or Safari)
- If Users need to use any other application, they should make contact with IT Support so the application can be assessed prior to using it to access WaterBear Information Resources.
- All unused, default User accounts must be removed/disabled from the device.
- All User accounts on the device must have passwords in place that meet the WaterBear Password Policy requirements (see earlier section of this document).
- On devices such as laptops and PCs and if the device is shared, the WaterBear User must set up a separate profile to access WaterBear Information Resources. IT Support can help with this if needed.
- Any unused applications used to access Company data must be removed from the device or disabled.
- Any unsupported/unsigned applications must be removed from the device.
- All applications must be kept up to date with the latest patches and security updates.
- Devices must be kept up to date with the latest OS and security updates available, which must be installed within 14 days of release.
- It is prohibited to access Company data using a rooted/jail-broken device.

8.3. **Security.** The security of WaterBear information and data is paramount. Users must not do anything which might compromise that security when using their own devices.

- The device must be password or PIN protected. The employee should not share the password or PIN with anyone.
- All passwords should be a mix of characters (as set out in the Password Policy).
- The device should lock after it has been left unattended for more than five minutes.
- WaterBear Users should ensure that any work product updated or created on a personal device is saved back to the suitable WaterBear online repository (e.g. SharePoint, Teams or OneDrive) and that data is not stored on the personal device any longer than is strictly necessary.
- If the device is lost or stolen, the employee **must** inform IT Support immediately and always within twenty-four hours. It might be necessary for IT Support to remotely wipe the device clean. If this does happen, there is no guarantee that personal information will not be deleted, although every effort will be made to avoid this.
- When a device is no longer being used, all WaterBear data and information must be deleted from the device. IT Support may be asked to check that this has been carried out thoroughly.
- Personal data relating to other staff members, tutors and students must never be stored on a personal device.

8.4. **Cost of Personal Device(s).** The device is the User’s property and always remains the property of the User.

- Users are advised to download and sign-in to the Microsoft Teams mobile application to be able to make and receive messages using their assigned WaterBear Teams account, on their personal device.

8.5. **Leaving WaterBear.** When a staff member or tutor leaves WaterBear, they must ensure that any WaterBear information has been removed from their personal device(s).

- Upon leaving the employment of WaterBear, the User’s account and associated access to company resources will also cease. This will be enforced through technical measures and also apply to access to WaterBear Information Resources on personally owned devices.

9. Enforcement

9.1. Users found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and related civil or criminal penalties.

9.2. Any vendor, consultant or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.