AXE BRUE, PARRETT &
NORTH SOMERSET LEVELS
INTERNAL DRAINAGE BOARDS

GOVERNANCE

IT & MOBILE PHONE POLICY

Version 1.0

To be reviewed annually

1.0. Introduction

1.1. The Somerset Drainage Boards Consortium makes internet access, email, IT equipment and Mobile Phones available to its Employees where relevant and useful for their jobs.

1.2. The internet and emails are powerful tools that can bring significant benefits to the Boards. However, it is important every person at the Consortium who uses the internet understands how to use it responsibly, safely and legally.

1.3. This Policy:

a. Reduces the online security risks faced by the Boards.

b. Let's staff know what they can and cannot do online.

c. Ensures Employees follow good email etiquette.

d. Ensures Employees do not view inappropriate content at work or using Board-supplied equipment.

e. Helps the Consortium satisfy its legal obligations regarding internet and email use.

1.4. This Policy should be read alongside other key Policies and Procedures. The Board's Data Protection Policy is particularly relevant to staff who use the internet and email.

1.5. This Policy applies to all Board Members, Staff, Consultants, Contractors, Students and Interns at the Consortium who use the Consortium's Internet, Email, IT or Mobile Phone equipment at any time.

1.6. This Policy applies to the use of the Internet and Consortium email on any device that is owned by the Consortium, or that is connected to any Consortium network or system.

2.0. Context

2.1. This Policy ensures the general security of our IT system whether users are accessing it from a desktop, laptop or mobile device. This Policy refers to Board-owned PCs, laptops and mobile devices as well as private user devices when used for Board business.

INFORMATION TECHNOLOGY & EMAIL

3.0. IT Equipment

3.1. This Policy document is applicable to all SDBC and private Desktop PCs, Laptops, Tablets and Mobile Phones that connects to the SDBC Server.

3.2. Employees should take all necessary measures to minimise loss of or damage to all Consortium IT assets in their use or control and protect those items from threats and environmental hazards.

3.3. Any IT equipment provided by the Consortium for use by Employees should be treated with care and not used for purposes it was not intended.

3.4. All equipment should be used in accordance with the manufacturer's instructions.

3.5. When used in-the-field, particular care should be taken with mobile devices and laptops to protect them from damage at all times.

3.6. Laptops must be securely stored when removed from the office (i.e., out of sight and in a locked boot of a vehicle) and never left in vehicles overnight.

3.7. Private user devices, when used for Board business, should apply all the same principles for safety and security of data as Consortium equipment.

4.0. Employees

4.1. Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need, e.g., systems or database administrators.

4.2. New Starters:

a. A member of the IT team will send a New Starter proforma to our IT support provider every time we request setup of a new user on the computer system.

b. Any set-up temporary password will only be used by the user to log-on for the first time at which point the user will be forced to set their own unique password.

4.3. Leavers:

A Leaver's proforma will be sent to our IT support provider every time we request removal of a User's access from the computer system;

a. Board-issued Smart Phones and other mobile devices will be returned to the Board prior to, or on the day of, departure.

b. The account password of a Leaver will be changed on the day of their departure in order to prevent any further access by the user to the computer system (including remote access).

c. The User's mailbox will be exported within 10-days of their departure; this will be stored in a central location on the server as a PST file so it can be made available to Management, as and when, for the purposes of checking legacy e-mail data.

d. The User account of a leaver will be deleted once the mailbox archive is complete.

e. IT team to evidence removal of accounts on personal devices on last working day.

5.0. Monitoring System Access and Use

5.1. Consortium email, IT and internet resources – including computers, smart phones, mobile devices and internet connections – are provided for legitimate business use.

5.2. The Consortium reserves the right to monitor use of email and the internet, to examine systems and review the data stored on those systems.

5.3. Examinations or monitoring of IT equipment and systems will only be carried out by authorised staff.

5.4. All internet data or emails written, sent or received through the Consortium's computer and email systems are part of official Consortium records. The Consortium can be legally compelled to show that information to law enforcement agencies or other parties under the Freedom of Information Act.

5.5. Users should always ensure that the business information sent via email, over, or uploaded to the internet is accurate, appropriate, ethical, and legal.

6.0. Password Policy

6.1. Default passwords are to meet the criteria in 6.2:

6.2. All passwords will comply with the following requirements:

a. Minimum password length = 8 characters (upper, lower, numeric & special character)

b. Password must meet complexity requirements = True

c. Maximum password age = 90 days

d. Minimum password age = 1 day

e. Passwords remembered = 24

f. Account lockout threshold = 6 invalid logon attempts

g. Account lockout duration = 5 minutes

6.3. When choosing your password:

a. Users should avoid choosing obvious passwords (such as those based on easily-discoverable information).

b. Common passwords must be avoided (SDBC, password, etc.)

c. Passwords must not be disclosed to anyone.

d. Passwords must be memorised, not recorded.

7.0. Protection from Malicious Software

7.1. Users must ensure that malicious software countermeasures are enabled on equipment and do not lapse. The IT System Administrator (GIS Officer) can advise on this and should be the first point of contact.

7.2. Users must be diligent regarding threats, reporting any suspicious emails to the SDBC IT System Administrator.

8.0. Security Scanning and Updates

8.1. Every Tuesday, users will log off but leave PCs and laptops running to allow overnight local scan.

8.2. An external vulnerability scan is included as part of IT Governance's Cyber Essentials package which will be renewed annually.

8.3. Users of Windows 10 computers should install updates at a convenient time but without excessive delay, as and when prompted by Windows.

8.4. Server updates are to be installed by Orchard IT support.

8.5. All users with Board owned mobile devices (smartphones & tablets) to install OS and APP updates without excessive delay as and when prompted.

8.6. All users with Board owned mobile devices should not alter the default settings and should allow their device to continue automatically downloading OS and APP updates in the normal way.

9.0. Removable Media

9.1. Removable media that contains data only, is to be virus-checked by the User prior to uploading to the network.

9.2. Any file with executable software will be unable to be transferred to the network due to the current Whitelisting restrictions. This will require the approval of the ICT Controller (Clerk or Deputy Clerk) before being authorised for use. Users breaching this requirement may be subject to disciplinary action.

10.0. Accreditation of Information Systems

10.1. All new information systems, applications and networks must be approved by the ICT controller before they commence operations.

11.0. Business Continuity and Disaster Recovery Plans

11.1. Risks to business continuity associated with IT are identified on the Risk Register. Users must familiarise themselves with the Risk Register and report any concerns to the SDBC IT System Administrator. Appropriate controls can then be implemented and documented and measures put in place to mitigate against loss or damages.

12.0. Wi-Fi

12.1. Separation of corporate Wi-Fi network (CORP) and the guest Wi-Fi network (GUEST) is to be maintained, and only Board-owned devices may be connected to the corporate network.

12.2. All staff personal and visitor devices may only may be connected to GUEST Wi-Fi.

13.0. Unsupported Operating System

13.1. PCs and mobile devices running unsupported operating systems shall NOT be allowed on the network.

14.0. Internet and Email Use

14.1. The Consortium recognises that the internet is an integral part of doing business, and that email is a key communication tool. It therefore encourages its Employees to use the internet and email responsibly whenever such use supports the Board's goals and objectives.

14.2. Only people who have been authorised to use the SDBC internet and email network at may do so.

a. Authorisation is usually provided by an Employee's Line Manager or the Chief Executive. It is typically granted when a new Employee joins the Consortium and is assigned their login details for the Consortium IT systems.

b. Unauthorised use of the Consortium's internet connection and email system is prohibited.

c. Employees who use the internet and email without authorisation – or who provide access to unauthorised people – may have disciplinary action taken against them.

14.3. The Consortium recognises that internet and email are embedded in many people's daily lives. As such, it allows Employees to use the internet and their Consortium email account for personal reasons, with the following stipulations:

a. Personal internet use should be of a reasonable level and normally restricted to non-work times, such as during lunch.

b. All rules described in this procedure apply equally to personal internet and email use. For instance, inappropriate content is always inappropriate, no matter whether it is being accessed, sent or received for business or personal reasons.

c. Personal internet and email use must not affect the internet and email services available to other users in the Consortium. For instance, downloading large files, streaming video or sending exceptionally large files by email, which could slow access for other Employees.

d. Users may access their own personal email accounts during their lunch break.

14.4. Users of the Consortium internet and email systems must not:

a. Knowingly introduce any form of computer virus, Trojan, spyware or other malware into the Consortium.

b. Disable security or email scanning software. These tools are essential to protect the Consortium from security problems.

c. Gain access to websites or systems for which they do not have authorisation, either within the business or outside it.

d. Send confidential Consortium data via email. The Chief Executive can advise on appropriate tools for this purpose.

e. Access another user's Consortium email account. If they require access to a specific message (for instance, while an Employee is off sick), they should approach their Line Manager or the Chief Executive.

f. Consortium data should only be uploaded and shared to the internet via approved services. The Chief Executive or IT System Administrator can advise on appropriate tools for sending and sharing large amounts of data.

14.5. Staff members must always consider the security of the Consortium's systems and data when using the internet and/or email. If required, help and guidance is available from Line Managers, the IT System Administrator and the Chief Executive.

14.6. Users should note that email is not inherently secure. Most emails transmitted over the internet are sent in plain text. This means they are vulnerable to interception. Although such interceptions are rare, it is best to regard email as an open communication system, not suitable for confidential messages and information.

14.7. There are many sources of inappropriate content and materials available online. It is important for Employees to understand that viewing or distributing inappropriate content over the internet, or by email, is not acceptable under any circumstances.

14.8. Users of the Consortium internet and email systems must not:

a. Take part in any activities that could bring the Consortium into disrepute.

b. Create or transmit material that might be defamatory or incur liability for the Consortium.

c. View, download, create or distribute any inappropriate content or material.

d. View, download or show content that may cause offence to other people.

14.9. Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

14.10. This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law such as;

a. Use of the internet or email for any illegal or criminal activities.

b. Broadcast of unsolicited personal views on social, personal, religious or other non-business-related matters.

c. Sending offensive or harassing material and/or emails to others.

d. Sending or posting messages or material that could damage Consortium's image or reputation.

Any user who receives an email or views content they consider to be inappropriate should report this to their Line Manager or the Chief Executive.

14.11. Emails are often used to communicate with rate payers, external partners and other important contacts. Although a relatively informal medium, staff should be aware that each email they send does affect the Consortium's image and reputation. Users of the Consortium email system must follow these rules of 'Best Practice':

a. Use the 'BCC' (blind carbon copy) field to send group messages to any groups that contain private email addresses or to members of the public. It stops an email recipient seeing who else was on the email circulation list, otherwise we risk infringing the Data Protection Act and GDPR.

b. Only use the 'Important Message' setting sparingly for messages that are really important.

c. Be sparing with group messages, only adding recipients who will find the message genuinely relevant and useful.

d. Always use a meaningful subject line rather than leaving it blank or using a single word like 'hello'.

e. Do not forward chain emails or 'humorous' messages. These clog up people's in-boxes and some topics are not appropriate for the workplace.

14.12. Email is a valid way to communicate with colleagues internally within the organisation, however it can be overused for internal communication. Users should keep these points in mind when emailing colleagues:

a. Would the issue be better addressed via a face-to-face discussion or telephone call?

b. Is email the best way to send a document out for discussion? Often, it becomes very hard to keep track of feedback and versions.

c. It is rarely necessary to 'reply all'. Usually, it is better to reply and then manually add other people who need to see a message.

d. Links to internal documents should be used for communication between staff wherever possible, rather than attachments.

15.0. Use of Private Equipment for Home-Working

15.1. Where homeworking is permitted, any device used to connect to the Board's Server must meet the standards required under Cyber Essentials (or equivalent accreditation) and this Board IT Policy.

15.2. Requirements may include, but not be limited to, OS / iOS version and Build status, an enabled Firewall and up-to-date Antivirus Software installation.

15.3. If a Staff member intends to use a new or replacement device for home working, they must confirm with IT support that it meets the required standards before attempting to connect to the SDBC Server.'

16.0. Copyright

16.1. The Consortium respects and operates within copyright laws.

16.2. Users of the Consortium internet and email systems must not:

a. Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.

b. Download illegal copies of music, films, games or other software, whether via file sharing services or other technologies.

c. Use the Consortium equipment, software or internet connection to perform any tasks which may involve breach of copyright law.

16.3. Users should keep in mind that the copyright on letters, files and other documents attached to emails may be owned by the email sender, or by a third party. Forwarding such emails on to other people may breach this copyright.

17.0. Social Media

17.1. This section provides guidance for Employee use of social media, which includes blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit uses to share information with others in a contemporaneous manner.

17.2. The following principles apply to professional use of social media on behalf of the Boards as well as personal use of social media when referencing the Boards.

a. Employees must know and adhere to the Staff Handbook and other Board policies when using social media in reference to the Boards.

b. Employees should use their best judgement, avoiding posting material that is inappropriate, defamatory or harmful to the Board, its Employees and Rate Payers.

c. Although not an exclusive list, refer to sections 14.8.a, b and c for some specific examples of prohibited social media conduct, as well as content that can create a hostile work environment.

d. Employees are not to publish, post or release any information that is considered confidential. If there are questions about what is considered confidential, Employees should first check with their line manager or the Chief Executive.

e. Subject to applicable law, after-hours online activity that violates the Boards policies may subject an Employee to disciplinary action or termination.

f. If Employees publish content after-hours that involves work or subjects associated with the Board, a disclaimer should be used, such as: “The postings on this site are my own and may not represent the Board’s positions, strategies or opinions.”

g. Employees must keep the Board related social media accounts separate from personal accounts

18.0. Potential Sanctions

18.1. Users knowingly breaching this IT, Internet and Email Policy may be held personally liable. Employees who do so will be subject to disciplinary action, up to and including termination of employment.

18.2. Where appropriate, the Consortium will involve the police or other law enforcement agencies in relation to breaches of this policy.

MOBILE PHONES

19.0. Introduction

19.1. This section applies to all SDBC Employees and/or Contractors that have been issued with Board Mobile Phones. This part of the Policy should be read in conjunction with the IT Policy.

20.0. Device Care and Maintenance

20.1. It is the responsibility of the Employee/Contractor (Users) to reasonably protect and maintain the working condition of the device that they have been provided. Users may be held liable for the repair of any damage to any such device if found to be negligent or wilful.

20.2. Users must adhere to any SDBC Policies and Procedures relating to the use of the device they have been provided.

20.3. SDBC issued phones are primarily for business purposes only but may be used for private business providing any Data and/or Call charges are within the Bundle Allowance for the device.

21.0. Usage Guidelines

21.1. In general, devices should not be used when they could pose a security or safety risk, or when they distract anyone from work tasks.

21.2. Mobile Devices must not be used while driving or operating equipment/machinery unless via a suitable hands-free system which should only be used to answer the call whilst you find a safe place to park.

21.3. Employees are encouraged to avoid speaking on mobile phones within earshot of colleagues’ working space.

21.4. Employees must adhere to any prescribed device Usage Limits relating to the equipment in their care. If Users are expected to exceed limits, they are to inform their Line Manager immediately they become aware in order to try and mitigate additional charges.

21.5. Employees are expected to use their devices prudently during working hours in the following circumstances;

a. For making or receiving work calls in an appropriate place and situation to do so.

b. For other work-related communication, such as text messaging or emailing in appropriate places and situations.

c. To schedule and keep track of appointments.

d. To carry out work-related research.

e. To keep track of work tasks.

f. To keep track of work contacts.

21.6. Users are NOT permitted to:

a. Use non-work-related applications on devices (e.g., games) within working hours.

b. Use their device's camera or microphone to record confidential information.

c. Use their device in areas where its use is explicitly prohibited.

d. Download or upload inappropriate, illegal, or obscene material on a company device (Para 14.10 refers).

22.0. Limitations on Use

22.1. Employees receive (2GB) Data Limits and Unlimited Calls and Texts per month. Phone and device usage is reviewed monthly. Where excessive use has been reported, Employees may be requested to provide evidence of usage.

22.2. Additional costs are incurred by the SDBC for the following:

a. International texts and calls.

b. Calls to Premium Rate numbers.

c. Non-Geographical Numbers (i.e., 0844).

22.3. Any additional costs incurred may be re-charged to the mobile phone/device User if they are found to be non-work-related.

23.0. Disciplinary Consequences

23.1. Improper use of any SDBC owned mobile phones or contravention of this Policy may result in disciplinary action.

23.2. Continued use of mobile phones at inappropriate times or in ways that distract from work may lead to mobile phone privileges being revoked and/or disciplinary action being taken.

23.3. SDBC retains the right to monitor Employees for excessive or inappropriate use of their mobile phones.

23.4. Employees may face severe disciplinary action, up to and including termination, in cases where their misuse of an SDBC device:

a. Causes a security breach.

b. Violates SDBC Data Protection Policy.

c. Causes an accident.

d. Can be categorised as an illegal or dangerous activity.

e. Is used for the purposes of bullying or harassment.