ACCEPTABLE USE OF IT POLICY

JANUARY 2024

CONTENTS PAGE

1. PURPOSE

1.1 The purpose of the Acceptable Use of IT Policy is to ensure that the Company's data and information are kept safe and secure and that our IT assets are used effectively and ethically.

2. SCOPE

2.1 This is a group level policy that applies to all authorised users of Anglian Water Group Limited and its subsidiary companies' systems and data, with the exception of Anglian Water (Ireland) Limited and Wave Limited (and their respective subsidiaries which include Celtic Anglian Water and Anglian Water Business (National)).

2.2 The phrase 'system users' in this policy refers to employees, workers and Alliance partners who are authorised users as detailed in 2.1 above.

3. STATUS

3.1 This policy and procedure are subject to regular review by the Company and are updated as appropriate.

4. POLICY OWNER

4.1 Head of Employee Relations.

5. POLICY

5.1. Introduction

5.1.1 It is everyone's responsibility as system users of Company IT services to read and understand this policy. All system users are required to follow this policy in order to keep the Company's data and information safe and secure. Non-compliance with this policy may result in disciplinary action.

5.1.2 All company system users must complete the mandatory "Acceptable Use of IT" training available on Workday as soon as possible after starting with the Company or having been notified that refresher training is needed. The maximum time allowable for successful completion of training is 56 days from notification.

5.2. Compliance and Ethical Behaviour

5.2.1 System users are not permitted to create, download, forward or share content that is illegal, may offend or upset others or could bring the Company into disrepute.

5.2.2 To help keep system users and the Company safe, system users IT activity may be monitored. For further information refer to the Company's Employee Monitoring Policy.

5.2.3 It is important that system users use of IT is lawful, so any use of IT that contravenes the Computer Misuse Act is prohibited. For further information refer to the Computer Misuse Act here: https://www.cps.gov.uk/legal-guidance/computer-misuse-act.

5.2.4 Security and process controls are in place to protect the Company, system users and our customers; attempts to circumvent these are prohibited.

5.2.5 Using the internet, including social media, or Company IT assets for limited and exceptional personal use is acceptable, providing it does not interfere with a system user's performance, inconvenience others or adversely affect the performance of Company IT. Streaming of films, music or other data rich media content must not be carried out unless it is authorised. Any personal use must not include taking, storing or sharing inappropriate material (pictures or comments), which could cause either reputational damage to the Company or distress to others. The Company reserves the right, at its absolute discretion, to withdraw this privilege at any time and/or to restrict access for personal use. If access to a mobile phone or data for on-going, personal use is needed, system users are expected to have separate, private accounts which they fund privately. Use of Company IT assets and accounts for premium rate lines, personal subscriptions and gambling are not allowed.

5.2.6 To protect Company data and infrastructure, local installation onto IS managed devices and/or procurement of software is only permitted with the approval of IS. Downloading applications onto smart devices from the Company-managed Application Stores does not require permission providing they do not breach this policy in another way.

5.2.7 System users must not use Company computer equipment for any purpose that is not connected to the Company's business unless they have express permission to do so or they are making personal use of the system as permitted by this policy. The use of Company systems for commercial purposes other than the business of the Company is strictly prohibited.

5.2.8 To help system users identify potentially malicious phishing emails, phishing simulation tests are carried out on a monthly basis. These tests are reinforced through the use of an escalatory process, whereby remedial training is provided to those who fail the tests, either on a single or on multiple occasions. Repeated failure of phishing simulation tests may lead to disciplinary action.

5.3 Data and Devices

5.3.1 With the approval of line management, home working and Bring Your Own Device (BYOD) are permitted. To do this securely system users must use the Company's approved solutions, which are:

- A Company issued and supported Mobile Device (Phone, Laptop, Tablet) with access via the Citrix VPN (for roles that require it) or direct access to Office 365 services.
- A Personal device compliant with the BYOD Policy accessing the virtual Citrix Virtual Desktop via https://agile.anglianwater.co.uk.
- A Personal device compliant with the BYOD Policy accessing Office 365 services via https://anglianwater.sharepoint.com or https://office.com.

5.3.2 In accordance with the Ways of Working revised hybrid/agile working policies, prior to home working system users are responsible for ensuring that they have suitable broadband and wireless or LAN connection at an appropriate speed. Company-

issued or system user mobile devices should not be tethered for this purpose. For absolute clarity, system users may not tether to corporate devices when working at home or away from a main site for significant periods of time; excessive data used in this way is in breach of the policy and may result in disciplinary action being taken.

On Fixed Sites

5.3.3 Tethering of devices to mobile phones on company sites should be done only if WiFi is not available and the issue has been reported to the IS Service Desk.

5.3.4 Connecting personal devices to the corporate network via "red cable" can result in damage to the Company network and is not allowed.

Company Mobile Devices

5.3.5 Data usage should be at a reasonable level for a system user's job role and excessive usage will be monitored. The Company reserves the right to take appropriate disciplinary action for any breach of this policy and procedure.

5.3.6 International Roaming (calls and data) is switched off by default for all Company devices. In exceptional circumstances, where there is a business- critical need, system users, by exception, may request that international roaming is switched on for their work device.

5.3.7 Requests for International Roaming to be switched on must be made in Workday by going to Requests > International Roaming and completing the form. The form will be sent for line manager approval before being sent to IS for activation.
Once activated, system users are fully responsible for charges and should remain aware and:

- use Wifi wherever possible to minimise the amount of call time/data used;
- only use the device for business-critical purposes;
- not use the device for any personal use such as calls, messaging or streaming using international roaming;
- be mindful of all charges, being vigilant and observant of charge notifications;
- accept full responsibility for any charges incurred to their cost centre; and
- agree to paying the charges for any inadvertent or personal use.

5.3.8 In the event that a Company laptop, Toughbook or desktop is reallocated from one individual to another this change must be notified to the service desk before reallocation.

5.3.9 Mobile phones should be replaced at end of life only, unless faulty/damaged or if increased functionality of a new phone is essential for an employee's job role. As a guide, mobile phones should last an absolute minimum of 2 years and considerably longer for most mobile phones.

5.3.10 Numbers will be barred with immediate effect when an individual leaves the Company and will be ceased 30 days later unless the manager of the individual requests, via the helpdesk, that the number be transferred to the new job holder.

Data and Information Handling

5.3.11 System users who need to share data outside of the Company must ensure that the data is adequately protected. Corporate tools such as OneDrive or SharePoint should be used, and Office Documents should be encrypted before sending. If it is not possible to use these tools, an encrypted USB memory stick can be requested, subject to approval by the relevant Data Protection and Information Security Forum representative. OneDrive is for personal use and sharing with others and should not be used as a replacement for the corporate document management systems (Lighthouse).

5.3.12 Keeping the Company's personal data and sensitive data safe is a legal obligation imposed by the Data Protection Act 2018 and the UK General Data Protection Regulation. E-mails containing Company sensitive data, such as personal data or customer data, must not be forwarded to personal e-mail addresses. If this information needs to be sent to a third-party corporate e-mail address, it must be protected appropriately.

5.3.13 In accordance with the Company's mandatory compliance to the Payment Card Industry Data Security Standards (PCI-DSS), account data such as unprotected card number (PAN), expiry date and CVV are not to be stored or transmitted via end-user messaging technologies (e.g. email, instant messaging, SMS or chat) under any circumstances.

5.3.14 Sensitive and confidential documents must be handled appropriately when sent for printing, to prevent a potential personal data breach. When sending to print, system users **must** pick up their documents straightaway or as soon as possible and **must** make sure that all pages are collected, and nothing is left on the printer. If there's a jam or the printer's out of paper, system users must sort the issue with the printer rather than send the document to print again as the sensitive, confidential documents may be held in the printer memory for someone else to print out and read. If system users cannot fix the printer issue, they **must** cancel the request to print before resending the print job to another printer.

5.3.15 Whilst the Company has limited control over personal devices (such as through the BYOD Policy), under no circumstances should the Company's information be downloaded or stored on personal devices outside of the restrictions within Office 365 or Citrix remote desktop. The BYOD policy provides further advice and guidance.

5.3.16 Where BYOD used for Company working is accessible and used by other family members, system users must ensure that they log out of and close any access to Office 365 and Citrix Remote Desktop when they finish working.

5.3.17 If system users need to copy data off the network onto portable media, such as portable hard drives or USB devices, the device must be a Company issued encrypted device.

Email

5.3.18 Employees must not send or forward mail messages that:

- contain information that could damage an individual, personally or professionally, e.g. defamatory messages; and/or
- damage Company intellectual property; and/or
- contain confidential information; and/or
- are illegal, would be considered offensive, or would bring the Company into disrepute.

5.3.19 Email auto-forwarding to internal accounts is permitted (e.g. from account1@anglianwater.co.uk to account2@anglianwater.co.uk). Auto-forwarding an employee's Company e-mail to an e-mail address that does not end in @anglianwater.co.uk or @AWG.com can result in the failure of the Company e-mail services. Where auto-forwarding of an @anglianwater.co.uk or @AWG.com mail account is established by a user, this must be only to organisations for which the Company has a completed, reviewed and approved Cyber Security Assessment in place to assure data security. The Company's Cyber team will monitor where e-mail auto-forwarding is set up and approve where a valid Cyber Security Assessment exists.

5.3.20 Company email must be used by all system users for Company business. Alliance Partners are allowed to use their works email address (i.e. @capgemini.com) for AWS business.

5.3.21 Personal email accounts must not be used for Company business as there is no guarantee that they are safe and secure. If an employee's IT account is locked or suspended, they are out of the business due to ill-health, or if they do not have an IT account, correspondence from the business regarding their employment may be sent to a personal email address with consent from the employee.

5.3.22 Storage space for large, resilient systems is costly to the Company. Therefore, to ensure the efficient running of the Exchange service, all email users must keep their mailboxes within approved limits (5GB). Each user will have an archived email box size of 100GB. System users who have a genuine business need for a larger mailbox limit should contact the IS Service Desk via the form on MyIT to request a larger mailbox. Please note that increases are not unlimited and mailbox clean-ups are required.

5.3.23 Nothing written in an email message can be guaranteed complete privacy. System users should be aware that email messages that have been sent to others potentially:

- can be forwarded from recipients to other users of the email system;
- can be printed and ultimately read by anyone who sees the printed message;
- can be inadvertently routed to an individual other than the intended recipient (e.g. when the recipient has email delegates); and
- can be accessed by others if PCs/laptops are unattended while log-in is active, which is a breach of the security policy.

5.3.24 System users must not access and/or store email files and messages that they are not authorised to view. System users must not forward mail messages and attachments that contain information that the recipient is not authorised to view. System Users must not post/send anonymous messages or pose as another user.

5.3.25 It is the responsibility of system users to read, understand and comply with the Data Classification Policies and Safe Information Handling guidance and to handle all data/information accordingly, (i.e. Sensitivity Labelling files). The Data Classification Policy and Safe Information Guidance are available on Lighthouse.

5.4 Securing Company Assets

5.4.1 It is a system user's responsibility to manage passwords and to keep them secure. This means not writing them down, re-using them or sharing them with anyone. If system users need to share access to a system, delegated privileges must be used and access requested for the colleague. System users who find it difficult to remember passwords may store them securely, for example in a password protected file. However, this file name **must not** contain any reference to words such as "passwords", "credentials" or "confidential" to prevent obvious identification of sensitive access credentials leading to inadvertent disclosure.

5.4.2 Physical security of assets is a system user's responsibility; system users must treat devices with due care and ensure that they are shut down and kept secure when in transit; system users should consider and be aware of the risks that can result from leaving Company devices unattended even at home. If system users need to leave devices in a vehicle for short periods of time, they must ensure that they are hidden from view and are not left in vehicles overnight. In addition, system users working from home on a Company device, must ensure the device is secured when not attended, (such as powered down or screen locked) to prevent others being able to access Company systems and/or data.

5.4.3 Changes required to IT access generated from new starters, moving job roles and leavers must be notified to IS promptly using the appropriate corporate processes.

Security Reporting

5.4.4 Any suspicious emails should be passed to the SPAMbin promptly, using the published process.

5.4.5 All security incidents, whether suspected or confirmed, must be reported promptly to the IS Service Desk.

5.5 Company Communication Channels

5.5.1 Microsoft Teams is the main communication channel and is the preferred option especially when compared to Whatsapp. Users should be aware that messages could be disclosable via a Data Subject Access request.

5.6 Privacy

5.6.1 Should system users use Company devices for personal use and information becomes available that there has been inappropriate use (taking, storing or sharing), the Company may request access to the device and to all associated personal material and personal accounts. If required personal material may be deleted without notice.

5.6.2 All data that is created and stored on Company devices is the property of the Company. There is no official provision for individual data privacy however, wherever possible, the Company will avoid opening personal e-mails or documents. It is an employee's responsibility when leaving the business to delete any personal data or documents they have created.

5.6.3 IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy.

5.6.4 The Company has the right, under certain conditions, to monitor activity on its systems in order to ensure system security and effective operation, and to protect against misuse. This includes the use of internet and e-mail.

5.6.5 Any monitoring will be carried out in accordance with audited, controlled internal processes, the General Data Protection Regulation (GDPR) and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

5.7 Video Recording Meetings

5.7.1 The meeting organiser must let people know, in advance, that the meeting is going to be recorded. This gives attendees the option to not appear in the recording. Attendees must raise any concerns with the organiser in advance. If an attendee does not want the meeting to be recorded, the meeting organiser should either not record the meeting or ask the attendee not to attend. It is important that:

- The meeting organiser **must** remind people that the meeting is being recorded when the meeting starts.
- Attendees, (except the meeting organiser), **must not** press record, even if this shows as an option.
- If there is a legal obligation to record the meeting, the organiser **mus**t notify all invitees about this and the reasons why the recording is required. (This only occurs rarely but is important to be aware of.)
- The meeting organiser **must** make sure the recording is kept securely – it is recommended to move this to a library in an appropriate SharePoint Team Site or publish this to an appropriate MS Stream channel if wider distribution is required.

The recording should be retained in accordance with the Company's Retention and Disposal Schedule.

5.8 Covert Surveillance

5.8.1 Generally, it is against the law to collect someone's information by filming them or otherwise recording them, without them knowing. This is called covert surveillance.

5.8.2 The Company does not permit, under any circumstances, covert or unauthorised audio/video recording by its employees. By way of illustration, covert surveillance would arise if an employee decided to secretly:

- video record a meeting with their manager on their mobile device;
- record the audio of a telephone conversation with a colleague;

- record a Teams meeting without telling all those attending that the meeting was going to be recorded and obtaining their agreement; and/or
- record a conversation with a customer or a trader, or a member of the public.

5.8.3 The Company will manage all incidents of alleged covert surveillance via the Company's Disciplinary Policy & Procedure.

FURTHER ASSISTANCE

Please contact your Line Manager or Employee Relations Manager/Advisor for further assistance.

LAST REVIEWED
January 2024