WATER MANAGEMENT ALLIANCE

GOVERNANCE

INFORMATION SECURITY AND SYSTEMS ACCEPTAPLE USE POLICY

BROADS IDB

EAST SUFFOLK IDB

KING'S LYNN IDB

NORFOLK RIVERS IDB

SOUTH HOLLAND IDB

Version: 1

Agreed Date: 23/03/2018

Review Date: 23/03/2021

The WMA and its member boards have a duty to preserve the confidentiality, integrity and availability of the information they hold to fulfil their statutory functions. The purpose of this policy is to ensure appropriate measures are put in place to protect this information and the integrated systems used to process it.

INFORMATION SECURITY AND SYSTEMS ACCEPTAPLE USE POLICY

Contents

Water Management Alliance

INFORMATION SECURITY AND SYSTEMS ACCEPTAPLE USE POLICY

1. Introduction

1.1 Our vision is to make each member board's district and watershed catchment area a safer place to live, work, learn, grow and have fun, a model of sustainable living in a high flood risk area. We aim to reduce the flood risk to people, property, infrastructure and the rural environment; become the local delivery partner of choice; enable & facilitate land use; and nurture, enhance and maintain the natural habitats and species which exist in and alongside our infrastructure.

1.2 To meet our aims and objectives the WMA and its member boards process and maintain information; financial, personal and some sensitive data pertaining to staff, ratepayers, board members and other companies. The WMA member boards have a duty to adhere to the Data Protection Act 2018 and the General Data Protection Regulation 2018. The boards are responsible for the protection, and integrity of this information and the systems used to process it. Unauthorized access to this data, IT systems and secured buildings can result in a loss of information, breach of confidentiality and action from the Information Commissioners Office (ICO).

2. Information Security and Systems Definition

2.1 This is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It is a general term that can be used regardless of the form the data may take (e.g. electronic or physical). Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data while maintaining a focus on efficient policy implementation, all without hampering organization productivity. (Source: Wikipedia (2018)).

3. Policy Aims

3.1 This policy has been put in place to protect the information used by the member boards and to ensure the correct and secure operation of assets used to process this information.

3.2 This policy applies to all the member boards' staff, board members, contractors and consultants using the board's information and assets. External consultants who independently use their own assets must state their Data Protection and Information Protection measures in their works contracts/bids.

4. Boards' Responsibilities

4.1 The employees of the WMA and its member boards, board members and others conducting business on behalf of the WMA and its member boards must comply with this policy.

4.2 Line Managers are accountable for the protection of information used by their staff and contractors; they must ensure staff and contractors are aware of this policy. Line managers will ensure all assets are returned upon the termination of employment or contract.

4.3 The Area Manager/Engineer is responsible for the procurement, technical security set-up, issuing assets and the maintenance of the asset register, in accordance with each Board's Financial Regulations.

4.4 The Data Manager must investigate, manage and resolve IT incidents and breaches. The Data Protection Officer (DPO) must report any breach within 72 hours to the ICO if it is considered that an information breach has occurred as a result. The DPO must communicate any breaches and changes in policies as a result to employees.

4.5 All employees must liaise and support investigations in the event of the theft of information and/or assets.

4.6 If you do not understand this policy or how it applies to you please seek advice from your Line Manager or the DPO. Failure to follow the rules set out in this policy could lead to disciplinary procedures or even a prosecution.

5. Equipment & Information Assets

5.1 All IT hardware must be ordered through the DPO or Data Manager. The hardware/assets are to be recorded on the hardware/asset register, including asset tags, serial numbers and the identity of the person to whom it has been issued.

5.2 Line Managers must ensure all assets are returned upon the termination of employment or contract. The returned assets will be checked and audited.

5.3 Hardware disposal, any data storage areas which are no longer fit for purpose must be physically destroyed.

5.4 Information asset owners must supply an accurate record when requested.

5.5 "Bring your own device" to work or BOYD; these devices are not to be connected to the boards IT network due to the potential security risk this can pose. If required the board can supply an encoded memory stick. The DPO or Data Manager may authorise the use of a personally owned device after an IT assessment has been carried out.

5.6 The board supplies identity badges, key fobs, and keys to boards' properties, to some employees. If these are lost or stolen it must be reported to your line manager as soon as possible.

6. Handling Information

6.1 Employees must ensure no unauthorised person has access to personal or sensitive data held by the board. Always lock your screen when leaving your workstation and try to avoid your screen being overseen by unauthorised individuals. Care should also be taken, not to be overheard when having discussions involving personal and sensitive data. No personal or sensitive data should be left on an answer machine; you don't know who has access to the recording.

6.2 All letters containing sensitive personal data must be sent either by hand delivery, recorded delivery or using a courier service.

6.3 Answering a request for personal or sensitive information must be authorised by the DPO or the Data Manger. The identity of the individual must be checked and proven before the information can be released, verbally, electronically or on paper.

6.4 No personal data is to be faxed.

6.5 When transporting data between sites using encrypted memory sticks. Notebooks and documents should be clearly labelled with contact details so they can be returned, should they be lost.

6.6 Data requests, a data request form must be completed and sent to either the DPO or the Data Manager. A data protection assessment may need to be carried out dependant on the request or a Data sharing agreement may need to be drawn up.

7. Storage & Disposal of Information

7.1 Data should be stored on the WMA servers or back up media. If work has been saved to the local drive, this should be moved onto the WMA servers at the

earliest opportunity. This will reduce the risk of data loss and the data will be backed up.

7.2 Any portable electronic device (i.e. notebook, memory stick, mobile phone) supplied by the WMA where the security of the information held on the device is the responsibility of the person using the device. Data must be moved to the servers at the earliest opportunity.

7.3 Personal and sensitive data/documents must be kept out of sight when not in use and locked away overnight. The contents of locked storage cupboards along with the key holders must be recorded and kept in a separate location. If keys are lost or stolen this must be reported immediately.

7.4 Documents no longer required as stated in the Document Retention & Destruction Policy must be disposed of securely, using the cross cutting shredder for paper documents and a reputable IT disposal company for the electronic devices as advised by the DPO or the Data Manager.

8. Email Usage

8.1 Only approved email accounts may be used to conduct WMA business. Emails and attachments sent and/or received (from WMA email accounts or personal accounts) regarding WMA or its member boards business, become part of the WMA records and are therefore subject to Freedom of Information requests, Data Protection Rights and Environmental Information Regulations.

8.2 The legal status of an email is similar to written communication; care must be taken not to enter into any agreement that constitutes a contract, without consent from the DPO or the Chief Executive.

8.3 WMA email accounts are not to be used to run personal or private business.

8.4 Unless an employee has given their prior written consent, accessing another user's email account is forbidden. If access is required whilst an employee is absent, approval must be given by the DPO or the Data Manager.

8.5 Emails sent regarding WMA or its members boards must be clearly marked with the sender's name, title, and contact details; they must never be sent anonymously.

8.6 Users should never send emails which could be deemed inappropriate, offensive, abusive, obscene, threatening, defamatory or illegal. A user who is unsure about the appropriateness of an email should consult with their Line Manager before sending.

8.7 Personal and sensitive data/documents should not be sent via email unprotected. It should be sent via secure email delivery service or password protected and marked as 'Strictly Private & Confidential'.

8.8 Always ensure users in a distribution list are authorised to read the content of an email, before sending or replying.

8.9 Do not use email accounts to permanently store records or documents that are of high importance, these should be stored on the WMA servers.

8.10 To reduce the risk of virus and malware infection be aware of unsolicited emails. If received do not reply, open any attachments, click on any hyperlinks or forward to another user; these emails should be deleted immediately and reported to the Data Manager.

9. Social Media

9.1 Social media is a highly interactive platform through which individuals, communities and organizations can share, co-create, discuss, and modify user-generated content or pre-made content posted online. They introduce substantial and pervasive changes to communication between businesses, organizations, communities, and individuals.

9.2 The use of the WMA or its member boards' logo or branding on social media channels must be authorized; failure to do so may result in action under the disciplinary procedure.

9.3 Before using social media as a channel for a project or campaign, an employee must first discuss and agree this with their Line Manager. All employees must not post any unchecked items on sites until it has been reviewed by another person, to avoid unintentional errors being posted.

9.4 Social media posts must not include contact details or images of people without their permission. Do not reveal confidential or sensitive information - consult the DPO or the Data Manager if you are unsure.

9.5 Never use comments that could be interpreted as offensive or defamatory, this could result in action under the disciplinary procedure. If the defamatory statement is written down (in print or online) it is known as libel. If it is spoken, it is known as slander. Action can also be taken against anyone repeating libelous information and defamatory statements from another source; careful checks are needed before quoting statements from other blogs or websites. This can also apply to linking to defamatory information.

9.6 The following social media activities are illegal under the Consumer Protection from Unfair Trading Regulations:

- Creating false blogs, or ghosting
- Falsely representing oneself as a customer
- Falsely advertising on social media sites

10. Internet Usage

10.1 The internet is a primary source of infection, the employee is responsible for internet usage and must check whether a site is safe to use. Check with the Data Manager or DPO before downloading any software from the internet.

10.2 All WMA laptops and PC's have virus and Malware protection installed. If this does not appear to be updating automatically please report this to your Line Manager or the Data Manager. Certain categories of web-sites are automatically blocked when using WMA internet access. Employees must not use free Wi-Fi hotspots to connect to the internet.

10.3 If a virus is suspected, immediately unplug the equipment and disable the Wi-Fi from the network and notify the Data Manager.

11. Security Incidents and Breaches

11.1 A security incident is an event that may be a threat to information, personal information and/or sensitive information (electronic or other media) or computer security by unauthorized access to a system. An incident or anticipated incident must be reported immediately to either the DPO or Data Manager. Incidents and breaches will be prioritised, investigated and action taken to minimise any actual or potential risk to the WMA information systems.

P J CAMAMILE
DATA PROTECTION OFFICER