WATER MANAGEMENT ALLIANCE

DATA BREACH PROCEDURES

GOVERNANCE

Last review date: August 2024

To be reviewed annually

Next review date: August 2025

Reviewed by: Data Protection Officer

Adopted by:

Broads Internal Drainage Board
East Suffolk Water Management Board
King's Lynn Internal Drainage Board
Norfolk Rivers Internal Drainage Board
Pevensey and Cuckmere Water Level Management Board
South Holland Internal Drainage Board
Waveney, Lower Yare and Lothingland Internal Drainage Board

The reporting and managing of any personal data breaches affecting confidential, personal or special category data is paramount. This procedural document supplements the WMA Data Protection Policy and the Information Security & Systems Acceptable Use Policy, which together with the Data Retention and Destruction Policy demonstrates the WMA Member Boards commitment to protecting the privacy rights of data subjects. These procedures explain how personal data breaches will be dealt with.

GOVERNANCE

Contents

GOVERNANCE

1. Introduction

This procedure applies to each WMA Member Board's employees, members, volunteers, contractors and those instructed by the Board to provide a service or those with whom the Board has entered into a joint working arrangement. This procedure provides information and guidance to support each Board's work and activities when dealing with a data breach.

All employees have a responsibility for the information they generate, manage, transmit and use in line with the Data Protection Act 2018 (DPA) and UK General Data Protection Regulation (GDPR). It is their contractual duty to secure personal and confidential data at all times. Any person who knows or suspects that a breach of data security has occurred should report the breach immediately in accordance with the WMA Member Boards Data Protection Policy.

Notifying the Information Commissioner's Office (ICO) of a personal data breach must be done without delay where feasible and no later than 72 hours after becoming aware of a breach. In the event that the data breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, organisations must also inform those individuals affected without undue delay.

Under the GDPR, records of any personal data breaches must be maintained, regardless of whether or not you are required to notify the ICO that the breach has taken place.

2. Purpose

The purpose of this procedure is to ensure that the provisions of the DPA and GDPR are complied with when managing a personal data breach.

This policy and guide supplements the WMA Member Boards Data Protection Policy which collectively demonstrates each Board's commitment to protecting the privacy rights of data subjects in accordance with the DPA and GDPR.

If the Board fails to notify either the ICO or where appropriate the data subjects affected by a data breach or both, the Board could have to pay an administrative fine. The value of this can be up to 10,000,000 EUR or up to 2% of the total revenue. A failure to notify a breach could demonstrate that there are no existing security measures or a lack of existing security measures. In that situation, the ICO will be able to issue sanctions for failure to notify or communicate the breach, and also absence of (adequate) security measures, as they are two separate infringements.

Accordingly, the WMA Member Boards have an important role to play when following the data security breach procedure, enabling each Board to comply with the DPA and GDPR, and avoid hefty fines.

3. What is a personal data breach?

A personal data breach is 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed' (Art 4 of GDPR). One of the consequences of a personal data breach would be the Board being unable to ensure compliance with the confidentiality and integrity principle as outlined in Article 5 of the GDPR. Breaches can be categorised based on the following information security principles;

- Confidentiality breach – where there is an unauthorised or an accidental disclosure of, or access to, personal data.
- Integrity breach – where there is an unauthorised or an accidental alteration of personal data.
- Availability breach – where there is an accidental or an unauthorised loss of access to or, destruction of, personal data.
- Loss or destruction breach – where personal data is lost or stolen.

Depending on the circumstances, a breach can affect confidentiality, availability and the integrity of personal data at the same time, as well as any combination of these. Such personal data security breaches could include the following examples:-

- disclosing confidential data to unauthorised individuals;
- loss or theft of portable devices containing personal or special category personal data e.g. laptops, PCs, mobile phones, USBs, disks, etc.;
- loss or theft of paper records;
- inappropriate access controls on electronic folders/files/drives which allows unauthorised access/use of personal data;
- suspected breach of the WMA Member Boards Data Protection and Information Security and Systems Acceptable Use policies;
- attempts to gain unauthorised access to computer systems e.g. hacking;
- records altered or deleted without appropriate consent/authorisation from the data subject;
- viruses or other attacks on ICT equipment, systems or networks;
- breaches of physical security e.g. breaking into secure rooms or filing cabinets where confidential personal data is stored;
- confidential personal data left unlocked in accessible areas;
- unsecure disposal of confidential paper waste;
- leaving PCs unattended when logged on to a user account without locking the screen to stop others accessing information;
- disclosing passwords to colleagues or others who could then gain unauthorised access to data;
- publication of confidential personal data onto the WMA Member Boards website or internet in error;

- misdirected e-mails containing personal, confidential or special category data.

4. What types of data do these procedures apply to?

These procedures apply to:

- all personal data created or received by the Boards in any format (including paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely;
- personal data held on all the Boards IT systems managed centrally by the external IT support company;
- any other IT systems on which the Boards data is held or processed.

5. Who is responsible for managing personal data security breaches?

Personal data security breaches are managed by each Board's Data Protection Officer (DPO) in conjunction with the ICT Manager where appropriate. In emergency data security breach situations the ICT Manager will manage the incident under the direction of the DPO.

6. Procedure for reporting data security breaches

In the event of a breach of data security occurring, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence.

If a personal data breach or potential or suspected personal data breach has been reported to you and/or you otherwise become aware of a personal data breach, please report this immediately to the DPO or ICT Manager. The attached Data Security Breach Report form should also be completed and e-mailed to the DPO DPO@wlma.org.uk as soon as possible after the initial reporting.

This report should record all relevant details of the incident and should be communicated to the Boards relevant staff on a strictly confidential basis to ensure that prompt and appropriate action is taken to resolve the breach incident.

- The DPO must then: Notify the ICT Manager and the Line Manager of the breach event;
- As stated in Article 33 of the GDPR, if the breach is likely to result in a risk to individuals the DPO must report the incident within 72 hours to the ICO;
- If the breach will impact and result in a risk to individuals, the DPO must also take steps to notify the individuals affected;

- If the DPO decides that the breach does not require to be reported to the ICO it should still be documented as a breach with an explanation justifying why it did not need to be reported to the ICO.

7. Managing personal data breaches

When managing a personal data breach the following five steps should be followed:

1. Identification and initial assessment.
2. Containment and recovery.
3. Risk assessment.
4. Notification.
5. Evaluation and response.

7.1 Identification and initial assessment

An incident or anticipated incident must be reported immediately to either the DPO or ICT Manager, using the form in Appendix A. The DPO will conduct an initial assessment to establish if a personal breach has taken place and what data has been involved/affected. The cause and extent of the breach, how many individuals have been affected. The level of harm/risk to the individuals and how the breach can be contained.

After the initial assessment the DPO will liaise with the departmental Line Managers associated with the breach to carry out a full investigation of the event. If the breach is significant, the DPO will also consider whether or not to establish a Breach Management Team made up of appropriate managers and/or third parties e.g. insurers or solicitors to assist with the investigation. All records relating to the investigation will be retained by the DPO.

The DPO will use the table below to determine the severity of the incident and this will be recorded on part 2 of the Data Security Breach Report Form. If the DPO deems the severity of the breach to be level 3 or above then the Board will be actively involved in the management of the event.

Breach Rating	**0 MINOR**	**1 LOW**	**2 HIGH**	**3 SERIOUS**	**4 SERIOUS**	**5 SERIOUS**	**6 ICO PENALTIES**
Board's Reputation	No significant impact on any individual/ group of individuals. Media interest very unlikely.	Damage to an individual's reputation or possible misuse of their personal data. Media interest possible.	Damage to a Board department's reputation. Media interest possible but it may not penetrate the public domain.	Damage to more than one Board department's reputation. Possible key local media coverage	Damage to Board's reputation. Breach impacts on >20 but < 50 data subjects. Local media coverage of breach.	Damage to Board's reputation. Breach impacts on >50 data subjects. National media coverage.	Breach will carry monetary penalty from ICO.

Data Subjects Potentially Affected	**MINOR** breach of confidentiality. Only a single data subject affected.	Breach is potentially serious but <10 data subjects affected and/or risk assessed as **LOW** e.g. files were encrypted.	Potential serious breach & risk assessed as **HIGH** e.g. unencrypted special category records lost. Breach impacts on <50 data subjects.	**SERIOUS** breach of confidentiality e.g. up to 100 data subjects affected e.g. loss of personal data relating to redundancies where data subjects clearly identifiable.	**SERIOUS** breach with either particular sensitivity /special category personal data e.g. medical records or up to 1000 data subjects affected.	**SERIOUS** breach with potential for identity theft and/or over 1000 data subjects affected.	**ICO PENALTIES.** Restitution to affected data subjects. Other liabilities such as systems updates/new software. Additional systems/ records Security. Legal Costs

7.2 Containment and recovery

Once it has been established that a data breach has occurred the respective Board must take immediate and appropriate action to limit the breach. Accordingly, the DPO with assistance from the ICT Manager will:

- Establish who needs to be made aware of the breach and advise them what needs to be done to contain the situation;
- Establish if anything can be done to recover any lost data and limit the damage of the breach e.g. physical recovery of the records, restoration of the data via data back-up;
- Establish if it is appropriate to notify affected data subjects immediately i.e. where the risk/harm to the data subjects has been deemed as high/serious.
- If appropriate, inform the Police in cases which involve data theft or other criminal activity relating to personal data.

7.3 Risk Assessment

The GDPR advises there is an obligation to notify a breach, however, it is not always a requirement. As soon as the respective Board is aware of a breach, it is vital that a risk assessment of the breach is carried out to contain the incident.
In assessing the risk arising from a personal data breach, the DPO along with all relevant members of WMA staff, should consider the potential adverse impact on data subjects i.e. what is the likelihood of actual harm to the affected data subjects and how serious or substantial is the impact likely to be.

The DPO, along with the relevant Board's Line Manager of the department where the breach occurred, will review the breach report in order to assess;

- The risks and consequences of the breach for both the data subjects involved and for the Board.
- The risk for the affected data subjects i.e. adverse consequences of the breach and how substantial/serious it is and the likelihood of it recurring.

GOVERNANCE

- The risks for the WMA and its Member Boards are strategic and operational; compliance and legal; financial; business continuity; and reputational damage.

Consideration must be given to the following:

- What type of personal data has been involved in the breach?
- Was the data protected in anyway?
- What has actually happened to the data in question?
- If it has been stolen could the type of data be used for other purposes which would be harmful to the data subjects involved?
- How many data subjects have been affected by the personal data breach? It should not be assumed that the risks are greater where large amounts of data have been lost, however, this must be considered and scrutinised.
- Whose personal data is the subject of the breach i.e. is it WMA staff, Board Members or rate payers? This will, to some extent, determine the level of risk posed by the breach and will also direct the actions in mitigating the risks.
- What harm could come to the data subjects affected by the breach? Are there potential risks to their physical safety, financial security or reputation or a combination of these factors?

Personal data breaches that could cause high risk to the individual's rights and freedoms are situations where the breach may lead to physical, material or non-material damage for those individuals whose data has been breached. Examples of this type of damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach comprises personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related to security measures, such damage should be considered likely to occur.

The DPO should decide, where appropriate, what remedial action should be taken on the basis of the breach report to mitigate the impact of the breach and also to ensure that the breach does not recur.

The DPO will prepare an incident report which will set out, where applicable, the following:

- a summary of the security breach;
- the individuals involved in the security breach (such as the Board members, contractors, external clients);
- details of the information, WMA IT systems, equipment or devices involved in the security breach and any information lost or compromised as a result of the incident;
- how the breach occurred;
- actions taken to resolve the breach;
- impact of the security breach;
- unrealised, potential consequences of the security breach;
- possible courses of action to prevent a repetition of the security breach;
- side effects, if any, of those courses of action; and

- recommendations for future actions and improvements in data protection, as are relevant to the breach incident.

This report will then be provided to relevant officers of the Board impacted by the breach. All relevant risk registers must be updated in respect of the personal data breach. Significant risks will be reported to both the Consortium Management Committee (CMC) and the relevant Member Board accordingly.

7.4 Notification

After taking the above into consideration, the DPO and the other relevant officers of the Board involved in the management of the breach, will determine whether or not it is necessary to notify the breach to others. Those that may need to be notified are:

- the data subjects affected by the breach
- the Board members
- the Information Commissioner's Office (if the breach poses a risk to data subject/s)
- the Police
- the press/media
- WMA's solicitors
- WMA's insurers

If the breach may cause a risk to individuals, the breach must be reported to the ICO within 72 hours. When notifying the ICO, as a minimum, the notification must include:

- a description of how and when the personal data breach occurred;
- what personal data was involved;
- who are the data subjects involved;
- approximate number of personal data records concerned;
- the likely consequences of the personal data breach; and
- what action has been taken to respond to/resolve the risks posed by the breach.

Subject to certain exemptions, if the personal data breach causes, or is likely to cause, a high risk to the data subjects, it may be necessary to inform the data subjects. If it is deemed necessary to notify the data subject(s) of the breach, the DPO must provide the data subjects in plain and clear language information on :

- the name and contact details of WMA's DPO or other point of contact;
- the likely consequences of the personal data breach;
- the measures taken or proposed to be taken by the WMA to address the personal data breach, including where appropriate, measures to mitigate its possible adverse effects.

The DPO must also decide on the most appropriate method of notification of the breach based on the following:

- Are there a large number of data subjects involved?;
- Does the breach involve special category personal data?;
- Is it necessary to write to each individual affected?;
- Should legal advice be sought on the wording of the notification?

The DPO must also ensure that the notification has a clear purpose e.g. that it enables the affected data subjects to take the necessary steps to protect themselves e.g. through cancelling bank cards, changing passwords etc., to allow regulatory bodies to perform their functions, provide advice and deal with any complaints. The focus of any breach response plan should be on protecting individuals and their personal data.

Where a decision is taken that it is necessary to notify the ICO, this must be done by the DPO within 72 hours from the point that officers became aware of the incident. The WMA will be regarded as having become "aware" when the WMA has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. This will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish whether or not the personal data has been compromised.

Where precise information is not available (e.g. the exact number of data subjects affected), this should not be a barrier to a timely breach notification. The GDPR allows for approximations to be made in the number of individuals affected and the number of personal data records concerned as it recognises that controllers may not always have all details of the incident available during this initial period.

It is more likely this will be the case for more complex breaches, such as some cyber security incidents where, for example, an in-depth forensic investigation may be necessary to fully establish the nature of the breach and the extent to which personal data has been compromised.

Consequently, in some cases, the DPO will have to do more investigation and follow-up with additional information at a later point. This is permissible as long as the DPO provides reasoning for the delay. It should be noted that there is no penalty for reporting an incident that ultimately transpires to not be a breach.

The focus instead when reporting a breach should be directed towards addressing the adverse effects of the breach rather than providing precise figures of those affected. Thus, when it has become clear that there has been a breach, but the extent of it is not yet known, a notification in phases is a safe way to meet the notification obligations.

7.5 Evaluation and Response

Subsequent to a personal data breach the DPO, in consultation with the relevant members of the Board, will conduct a review to ensure that the steps taken during the incident were appropriate and to identify any areas for improvement.

GOVERNANCE

The DPO will maintain a central record of all breach occurrences. However, for any serious breaches the DPO will conduct a review and provide a detailed report to the WMA CMC stating:

- the action which needs to be taken to reduce the risk of future breaches to minimise their impact;
- whether any policies, procedures or reporting lines require improvement to increase the effectiveness of response to the breach;
- if there are any faults or weak points in security controls which need to be tightened up;
- staff awareness/training issues which would prevent recurrence of the breach;
- additional investment in resources/infrastructure to reduce exposure to breach and relating cost implications.

It is important to keep in mind that, regardless of whether or not a breach needs to be notified to the ICO, under Article 33(5) of the GDPR, the Board must keep documentation of all breaches comprising the facts relating to the personal data breach, its effects and consequences and the remedial action that was taken. The Board will also record its reasoning for the decisions taken in response to a breach, in particular, if the breach has not been notified, a justification for that decision made. This documentation will enable the Board to verify its compliance with the Regulation, as these records can be requested by the ICO. This is linked to the important accountability principle of the GDPR, contained in Article 5(2). Controllers, like the Board, are encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not. If the Board fails to adequately document this process, there will be financial penalties in accordance with Article 83.

8. Further Information

The Board is registered with the Information Commissioners Office (ICO) and pays an annual fee.

The Board has a Document Retention & Destruction Policy providing details of the periods for which documents/data are held.

The Board has an Information Security and Systems Acceptable Use Policy which provides details of the measures that have been put in place to protect information and the integrated systems used to process it.

The Board has a Privacy Policy which can be found on the web-site and/or supplied upon request.

Where a person wishes to raise a query, issue or complaint about how their personal information is, or has been, processed, they should, in the first instance be directed to the Data Protection Officer (see details below).

GOVERNANCE

9. Data Protection Officer: contact information

For information about how to request access to personal information please contact:

Data Protection Officer
Pierpoint House
Horsley's Fields
King's Lynn
PE30 5DD
Tel: 01553 819600
Email: DPO@wlma.org.uk

P J CAMAMILE
DATA PROTECTION OFFICER

Appendix A: Data Breach Questionnaire

Data Breach Questionnaire

Please answer the questions below; enter N/A if the question is not relevant or TBC if the question cannot be answered at present.

If you can identify someone else who may be able to answer any of the questions, please indicate this in your response.

Send the completed form to the Data Protection Officer at DPO@wlma.org.uk. **flagged as High Importance. You will be advised on further actions. If the breach is currently ongoing (i.e. data is still at risk or exposed), contact 01553 819600 or 07841 571251 as soon as possible.**

Date:	Your Name:	Contact: Email / Mobile

	Your answer	DPO notes
1. About the data breach		
When did this data breach occur?		
When did the IDB become aware of the data breach?		
How did you become aware of the breach?		
What do you think caused the breach? (e.g. human error, theft, cyber-attack)		
Where did this data breach occur?		
Please provide a brief description of the circumstances leading to the breach		
2. About the data		
Who would normally be responsible for the data?		

GOVERNANCE

	Your answer	DPO notes
Does any of the data relate to identifiable living individuals?		
What does the data consist of? Please provide a full description		
Were any of the following data types involved (if yes, tick all boxes that apply) * × Includes any inherited or acquired data which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question. † Any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, fingerprints, blood samples etc. ‡ Includes employment rates, crime rates, poverty status, education levels, life expectancy etc. ◊ Includes CVs, job application forms, job references, PDRs, development reviews, pension, payroll, sickness etc.	☐ Racial or ethnic origin ☐ Political opinions ☐ Religious beliefs ☐ Trade union membership ☐ Health data/medical data (physical or mental), well-being etc. ☐ Sexual life/orientation data ☐ Criminal offences ☐ Detail of proceedings relating to criminal offences ☐ Genetic data × ☐ Biometric data † ☐ Socio Economic Data ‡ ☐ Grades/Achievements/Personal Statements etc. ☐ Financial data, including account numbers, card details etc. ☐ Employment data ◊ ☐ None of the above	

GOVERNANCE

	Your answer	DPO notes
Does this incident/breach involve Commercially Sensitive Data? *	☐ Yes ☐ No If yes, what was the classification? * ☐ Public ☐ Protected ☐ Restricted ☐ Reserved ☐ None of the above	
Approximately how many individuals are affected?		
Was the data secured against unauthorised access? If so, can you describe how it was secured? E.g. Was the data encrypted? Who held the encryption keys? How were the encryptions keys kept secure?		
Do you know if anyone has had access to the data when it was no longer under your control? Please explain who might have been able to access the data		
Do you have a copy of the data that was lost?		
Have the staff involved in this data loss received Data Protection training, and if so, when?		
3. Actions since breach		
Have you attempted to get the data back from those who now hold it?		

GOVERNANCE

	Your answer	DPO notes
Have you informed the data subjects that this incident has occurred?		
Have you taken any action to minimise/mitigate the effect on the data subjects involved? If so, please provide brief details.		
Are you carrying out an internal investigation into the incident – If so when will you complete it and what format will it take?		
Have you informed any other regulatory body of the matter? If so, please provide their details and an outline of their response.		
What actions have you taken to prevent similar incidents in the future?		
Is there any other information you feel would be helpful to an assessment of the incident?		