Data Security Breach Reporting Procedure

1 Introduction

Data security breaches can occur in many ways including through human error or malicious intent.

Changing technology trends is resulting in the creation of more data and information in more dynamic ways. Inevitably therefore, there are more emerging ways for security breaches to occur.

Under the EU General Data Protection Regulation (GDPR), Data Controllers have an obligation to implement systematic processes for responding to breaches of the Personal Data they hold.

This Data Security Breach Reporting Procedure sets out the process for responding to any data security breach within Farnham Angling Society (FAS).

2 Aim

The aim of this policy is to standardise the approach and response of FAS to any allegation and /or reported data security breach incident, and to ensure that any such incident is appropriately recorded and managed and reported in accordance with best practice guidelines.

By adopting a standardised and consistent approach to all reported incidents, the aim is to ensure that:

- Incidents are reported efficiently and in a timely manner and can be properly investigated.
- Incidents are handled by appropriately authorised and skilled and competent personnel.
- Appropriate levels of FAS management are involved at the right time.
- Incidents are recorded and documented to a high standard.
- The impact of the incidents is understood and appropriate action is taken to mitigate or prevent further damage.
- Evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny.
- External bodies or data subjects are informed as required.
- The incidents are dealt with in a timely manner and normal operations restored as quickly as possible.
- The incidents are reviewed to identify areas for improvements in FAS operations, policies and procedures.

3 Definitions

3.1 Data Security Breach

A data security breach is considered to be "any loss of, or unauthorised access to FAS data". FAS data includes (but is not limited to) information about its business operations and activities, Members, Officers, suppliers and contractors.

Examples of data security breaches may include:

- Loss or theft of FAS data or equipment on which FAS data is stored
- Unauthorised access to and/or use of FAS confidential or highly confidential data
- Equipment failure and/or human error resulting in loss or misappropriation of data
- Unforeseen circumstances such as a fire or flood
- Hacking, cyber attacks
- Information obtained by fraud, deceit or through misrepresentation.

For the purposes of this procedure, data security breaches include both confirmed and suspected incidents.

4 Scope

This policy applies to all FAS information, regardless of format. It is applicable to all officers and contractors. It is to be read in conjunction with the FAS-IT Security Policy.

5 Responsibilities

5.1 Information users

All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

5.2 Senior Officers

Senior Officers are responsible for ensuring that Officers act in compliance with this procedure and assist with investigations as required.

5.3 Lead Responsible Officers

The Data Protection Officer (DPO) will be responsible for overseeing management of the breach in accordance with this procedure. Suitable delegation may be appropriate in some circumstances.

The DPO is the point of contact for the breach of data security.

The DPO for this organisation is Ian Gray.

5.4 Incident Management Team (Ian Gray, Deryk Randall, Mick Borra & Nik Turner)

An Incident Management Team (IMT) will be formed and be responsible for investigating incidents relating to the data security breach, maintaining records and reporting progress the DPO.

6 Data Classification

Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that FAS is able to quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner.

All reported incidents should include the appropriate data classification to assist with risk assessment. For the purpose of this policy, data is classified into Public data; Internal data; Confidential data and Highly confidential data.

6.1 Public Data:

Data intended for public use – this can be made public without any negative impact on FAS. This includes data relating to business activities, individuals and customers.

6.2 Internal Data:

Data regarding the day-to-day business operations of FAS. This is primarily for Senior Officers use.

6.3 Confidential Data:

Data about Members & Officers. Access should be limited to only those people that need to know as part of their role.

6.4 Highly Confidential Data:

Information that, if released, will cause significant damage to the business activities or reputation of FAS. E.g. Special Category Personal Data, financial information. Access to this information should be highly restricted. This includes data relating to Members and Officers.

7 Authority

Officers, contractors and consultants who act in breach of this policy or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

8 Data Breach Management Plan

The management response to any reported data security breach will involve the following four elements.

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Process Flow Diagram

DATA SECURITY BREACH

(suspected or confirmed)

If personal data is involved, notify the DPO **immediately**.

INFORM THE DPO:

Ian Gray – Registration Number A8395852.

GDPR-DPO@farnhamanglingsociety.com

DPO TO APPOINT INCIDENT MANAGEMENT TEAM (IMT)

IMT will log record of the incident and monitor progress /resolution

IMT TO INVESTIGATE INCIDENT

Using the Containment & Recovery Form, investigate the incident **quickly**.

It is important to progress quickly to investigation as Data Controllers must notify no later than 72 hours where a breach of personal data is likely to result in a risk to the rights and freedom of the data subject.

ASSESS THE RISKS

Using the Assessment of Risks Form, assess the risks.

CONSIDER FURTHER NOTIFICATION

Using the Consideration of Further Notification Form, consider notification options. At this point, it is important to **liaise actively** with DPO.

EVALUATE THE EFFECTIVENESS OF THE RESPONSE TO THE BREACH

Using the Evaluation and Response Form, evaluate the effectiveness of FAS to the breach.

REPORTING

Complete the Incident Report Form, send the completed form to DPO

ACTIONS

DPO to review the report from the IMT and consider recommendation(s) made and take appropriate steps.

Evaluation of Incident Security

The severity of the incident will be assessed by the DPO.
Assessment should be made based on the following criteria:

High Criticality: Major Incident	**Contact**
• Highly Confidential Data • Personal data breach that has been indicated would cause harm • External third-party data involved • Significant or irreversible consequences • Likely media coverage • Immediate response required regardless of whether it is contained or not • Requires significant response beyond normal operating procedures	DPO Other relevant contacts on approval from DPO: • Executive Committee members • Police • ICO • Data Subjects
Moderate Criticality: Serious Incident	Contact
• Confidential Data, classed as moderate by the business • Not contained within FAS • Breach involves personal data but at moderate risk of causing harm • Significant inconvenience will be experienced by individuals impacted • Incident may not yet be contained • Incident does not require immediate response	DPO Other relevant contacts on approval from DPO: • Executive Committee members • Police • ICO • Data Subjects
Low Criticality: Minor Incident	Contact
Internal or Confidential Data • Small number of individuals involved • Risk to FAS low • Inconvenience may be suffered by individuals impacted • Loss of data is contained/encrypted • Incident can be responded to in working hours Eg: Email sent to wrong recipient, mobile device lost	DPO Other relevant contacts on approval from DPO: • Executive Committee members • Police • ICO • Data Subjects

Containment and Recovery

Step	Action	Notes
	Containment and Recovery:	**To contain any breach, to limit further damage as far as possible and to seek to recover any lost data.**
1	Identify the cause of the breach.	
2	Establish what steps can or need to be taken to contain the breach from further loss.	
3	Contain the risk e.g. take systems offline or restrict access to a small number of staff until more is known about the incident.	
4	Contact all relevant Officers who may be able to assist in the process.	
5	Ensure that the possibility of further data loss is removed or mitigated to the best extent possible.	
6	Determine whether anything can be done to recover any losses and limit any damage that may be caused. This can include physical recovery of data / equipment or use of back-ups (where data is corrupted).	
7	Where appropriate, the DPO to inform the police / Data Subject / ICO.	E.g. stolen property, fraudulent activity, offence under Computer Misuse Act.
8	Ensure all key actions and decisions are logged and recorded on the timeline.	
9	Within 24 hours, send the Incident Report Form (Appendix 5) to the DPO by email	

Assessment of Risks

Step	Action	Notes
	Assessment of Risks	**To identify and assess the ongoing risks that may be associated with the breach.**
1	What type and volume of data is involved?	Data Classification/volume of individual data etc.
2	How sensitive is the data?	Sensitive personal data? By virtue of definition within legislation (e.g. health record) or sensitive because of what might happen if misused (banking details)
3	What has happened to the data?	E.g. if data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
4	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	E.g. encryption of data/device.
5	If the data was damaged/corrupted /lost, were there protections in place to mitigate the impact of the loss?	E.g. back-up tapes/copies.
6	The number of individuals' personal data affected by the breach?	
7	Whose data is compromised?	Member, Officer, contractors, suppliers etc
8	What could the data tell a third party about the individual? Could it be misused?	Consider this regardless of what has happened to the data. Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.

9	Is there actual/potential harm that could come to any individuals?	e.g. are there risks to: - Physical safety; - Emotional wellbeing; - Reputation; - Finances; - Identify (theft/fraud from release of non-public identifiers); or - a combination of these and other private aspects of their life?
10	Are there wider consequences to consider?	E.g. a risk to public health or loss of public confidence in an important service we provide?
11	Are there others who might advise on risks/courses of action?	E.g. If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

Consideration of Further Notification

Step	Action	Notes
	Consideration of Further Notification	**Notification is to enable individuals, who may have been affected, to take steps to protect themselves or allow the regulatory bodies to perform their functions.**
1	Are there any legal, contractual or regulatory requirements to notify?	Contractual obligations?
2	Can notification help the individual?	Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?
3	Due to the nature of the breach does the serious consequences require notification to inform the Information Commissioner's Office?	Consult the relevant ICO guidance on when and how to notify it about breaches. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
4	Consider the dangers of 'over notifying'	Incident may not cause harm, e.g. not able to identify a subject directly or indirectly
5	Consider whom to notify, what you will tell them and how you will communicate the message.	There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation. Include a description of how and when the breach occurred and what data was involved. Include details of what mitigation has been done to respond to the risks posed by the breach. When notifying individuals give specific and clear advice on the steps

		they can take to protect themselves along with what the institution is willing to do to help them. Provide a way in which they can contact us for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page).
6	Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.	E.g. police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.

Evaluation and Response

Step	Action	Notes
	Evaluation and Response	To evaluate the effectiveness of FAS Webmaster/System Administrator) and Heart Internet response to the breach
1	Establish where any present or future risks lie	Review procedures to address them.
2	Consider the data and contexts involved	E.g. what data is held, its extent, sensitivity, where and how it is stored, how long it is kept
3	Consider and identify any weak points in existing security measures and procedures	E.g. in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections
4	Consider and identify any weak points in levels of security awareness/training	Fill any gaps through training or tailored advice
5	Report on findings	Report to management team
6	Implement recommendations	
7	Evaluate Risk Assessment	Update and improve when required

Incident Report Form

Incident Report Form	
Description of the Data Breach	
Time and Date breach was identified and by whom	
Who is reporting the breach: Name/Post/Dept.	
Contact details: Telephone/Email	
Classification of data breached (as defined in this document under Data Classification) i. Public Data ii. Internal Data iii. Confidential Data iv. Highly confidential Data	
Volume of data involved	
Confirmed or suspected breach?	
Is the breach contained or ongoing?	
If ongoing, what actions are being taken to recover the data?	
Who has been informed of the breach?	
Any other relevant information	
Cause of the Data Breach	
Steps taken to contain / mitigate the breach	
Who has assisted with the process so far e.g staff / department?	
What steps have been taken to recover any losses and limit any damage?	
Details of the data: i. What type and volume of data is involved?	

ii. How sensitive is the data? iii. What has happened to the data? iv. If the data was lost / stolen, were there any protections in place to prevent access / misuse? v. If the data was damaged / corrupted / lost, were there protections in place to mitigate the impact of the loss? vi. The number of individuals’ personal data affected by the breach? vii Whose data is compromised? viii) What could the data tell a third party about the individual? Could it be misused? ix) Is there actual / potential harm that could come to any individuals? x) Are there other consequences to consider? xi) Are there others who might advise on risks / courses of action?	
Are there any present or future risks? If yes, explain:	
Have you considered the data and contexts involved? If yes, explain:	
Have you identified any weak points in existing security measures and procedures? If yes, explain:	
Have you identified any weak points in existing security measures and procedures? If yes, explain:	
Have you identified any weak points in levels of security / awareness training. If yes, explain:	
Conclusion/Findings/Recommendations Implementation	

Definition of Personal Data

The definition of personal data includes (but is not limited to):

- Personal details including name and contact information.
- Family and lifestyle details.
- Device details.
- User activity details and user preferences.
- Browser history details.
- Location details.
- Electronic identification data including IP address and information collected through cookies.
- Financial details.
- Credit card information and payment details.
- Contractual details including the goods and services provided.
- Special categories of personal data including biometric data.
- Date of birth.
- Gender.
- Marital status and dependants.
- Beneficiary and emergency contact information.
- Government identification numbers.
- Education and training details including professional memberships.
- Bank account details.
- Payroll information.
- Wage and benefit information.
- Car registration and insurance information and copy/details of driving licence.
- Documents supporting any visas required for business purposes.
- Performance information including performance appraisal records.
- Employment details.
- Any disciplinary, grievance and capability records.
- Annual leave and other leave records.
- Information about use of company IT systems.
- Photographs.
- Recruitment records.
- Health and safety records.
- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade-union membership.
- Genetics, biometrics or health records.
- Sex life or sexual orientation records.