Information Loss Handling Plan & Policy

This code should be reviewed every year

Date Agreed by Club Committee _____

Date for Review _____

Signature: …… Club Chair

Signature: …… Club Secretary

Table of Contents

1) Background

- One of the principles of the General Data Protection Regulations states that,

  > *"Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."*

- In practice, this means we must have appropriate security to prevent any personal data we hold being accidentally or deliberately compromised.

***Please refer to Annex A** which summarises the key security measures within the organisation to prevent or reduce data loss.*

- A data loss incident is defined as any instance or suspected instance of:
  - Accidental or deliberate disclosure of information (including loss of confidentiality);
  - Accidental or deliberate destruction, loss or modification of information (including loss / corruption and unauthorised changes to customer data); and
  - Theft of information.

2) Purpose

The purpose of this document is to set out the plan and arrangements that Newcastle Tennis Club to implement to report and handle loss of information, and to describe in broad terms the responsibilities of key personnel and the actions which need to be taken.

3) Definition of Minor and Major Incidents

Minor incidents

- Minor incidents include loss of smart cards, minor information compromises (i.e. single customer/staff record), etc.

Major incidents

- Major incidents include unauthorised access to IT systems; theft/ loss of organisational property/assets/information (Multiple records) and compromise of Information (Multiple records).
- If unclear whether the loss is minor or major, the Club Chairperson can advise.
- Consideration should be given to the exact nature of the information lost or breached, the protective marking it carries, the impact level for the information which has been compromised, the amount / volume and the timescale over which the release has occurred and if possible, the recipient (s) of the information.

4) Steps to follow when actual/potential data loss has been detected

a) Reporting the loss

REPORT:

- If data is actually/potentially lost or stolen, the person who first discovers the loss or theft must report it within the hour using the Data Loss Report template

Please refer to Annex B

OTHER ACTION REQUIRED:

- The report should be sent to the Club Chairperson.
- Where a loss is as a result of theft from or burglary from premises the incident must always be reported to the PSNI immediately.

b) Investigation

INVESTIGATION:

- Data security breaches/losses will require not just an initial response to investigate and contain the situation but also for major loss/breach a recovery plan including, where necessary, damage limitation.

The Club Chairperson should carry out an investigation of the data loss using the procedures set out in the template at ***Please refer to Annex C***

OTHER ACTION REQUIRED:

- The Club Chairperson should also assess the risk to determine the severity of the data loss. This may need to be revised as more information about the incident is gathered.
- Loss of personal data or sensitive personal data will increase the risk.
- Other factors which should be considered when assessing the seriousness of the consequences are ***set out in the risk assessment below***.

Risk category	Example of risk
Governance and culture	• Lack of comprehensive oversight and control • When something goes wrong, handling it badly and not learning • Third parties letting you down • New business services not taking information risk into account
Information management and information integrity	• Critical information is wrongly destroyed, not kept or cannot be found when needed • Lack of basic records management disciplines • Inaccurate information • Information becomes unreadable due to technical obsolescence • Information is lost or exposed

The human dimension	• Despite having procedures and rules, staff act in error, act incorrectly • Despite having procedures and rules, insiders act incorrectly. • External parties source your information illegally
Information availability and use	• Inappropriate disclosure of sensitive information • Failure to utilise the value of the information asset • Failure to allow information to get to the right people at the right times
Technology	• Denial of service due to systems failure • Corruption of data leading to delay in services
Process disruption	• Established processes disrupted by new regulation/processes
Proportionality	• Providing more information than necessary for completion of a process leads to the risk of a breach being more critical than it need be.

STEPS TO BE TAKEN:

- The Club Chairperson will consider incidents reported and advise on any steps to be taken.
- Any data subjects whose data has been lost or stolen may need to be informed. Factors to consider include:
  - *The amount of data*
  - *Was sensitive personal data lost?*
  - *Does it have the potential to cause harm?*
  - *Is it already in the public domain?*
  - *Can notification help the individual to mitigate further risk?*
- For more information about the specific breach notification requirements for service providers see www.ico.org.uk.

WHO ELSE MAY NEED TO BE CONTACTED?

- The PSNI may need to be informed if theft, fraud or any other criminal activity is suspected.
- The Information Commissioner's Office (ICO) may need to be informed where the loss is considered serious (for example, in the unlikely circumstances of large volumes of personal information being lost, or where personal data loss could cause a significant risk of individuals suffering substantial harm.)
- For further information on the circumstances in which the ICO expects to be notified of security breaches please contact the Information Commissioner Office www.ico.org.uk.
- Media: The ICO may recommend the data controller to make a breach public where it is clearly in the interests of the individuals concerned or there is a strong public interest argument to do so.

c) Response

The appropriate response will depend upon the type and volume of information lost.

It is important to keep in mind the principles of containment and recovery; assessing the risks, notification of breaches; and evaluation and response.

TEMPLATES TO USE

Annex D contains a template which should be used to record relevant findings as the incident unfolds. This will help inform decisions on actions which should be taken.

A recovery plan should be prepared and implemented without delay. A template is provided at **Annex E**.

As events unfold, decisions are made and actions are taken, they should be recorded. A template Event Log is provided at **Annex F.**

d) Evaluate

It is essential to evaluate the effectiveness of the response. This will help identify measures to prevent it happening again.

An information incident loss will highlight very starkly the vulnerabilities in information management that have led to the loss.

These could include, for example:

i. Little or no awareness of data protection principles;
ii. Systemic or ongoing problems;
iii. Inadequate policies or a lack of clear allocation of responsibility;
iv. Insecure electronic transfer of information; and
v. Unauthorised/ inappropriate release of personal data to third parties.

LESSONS LEARNT REPORT & ACTION PLAN:

It will be essential that any such issues identified, as a result of the investigation in the cause of the information loss, be acted on as soon as possible.

This should be achieved by a 'lessons learnt' report.

This should be then translated into an action plan which should be circulated to relevant committee members for the purposes of preventing similar future incidents.

Such an action plan should include a clear timetable.

ANNEXES

Annex A Arrangements to prevent or reduce data loss

The following security measures seek to ensure that only authorised people can access, alter, disclose or destroy data; those people only act within the scope of their authority; and if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.

Newcastle Tennis Club has a range of controls in place to prevent or reduce data loss and include the following. This list is not exhaustive

Physical controls

- Newcastle Tennis Club Computers are regularly updated with the latest antivirus software,
- Password protected systems and screen savers,
- All protectively marked information has to be locked away securely at the end of each day.
- All protectively marked information is destroyed on line with guidance

Procedural controls

- Club Office Clear desk policy
- Assets such as equipment, information, software, and digital cameras are only used by committee members and coaching contractors that have been given permission to do so.
- Laptops held in a locked filing cabinet/ cupboard when not in use.
- Only the minimum documentation or information required is taken off site and only when needed for business purposes.
- Procedures for responding to requests for information
- Data sharing agreements in place where data is shared with third parties
- Privacy policies and data security guidance for coaching contractors
- Use of protective marking and core descriptor to facilitate document handling, storage, transfer and disposal

Annex B Template Data Loss Report

Initial report of lost or stolen data

When data has been lost use this form to report the loss to management.

Describe what was lost:	
Did it contain personal data or sensitive personal data?	
How many records were lost or how many people are affected?	
Was the data lost, stolen or inappropriately disclosed?	
When did the loss occur?	
When was the loss discovered?	
Who discovered the loss?	
Where was the data lost or stolen?	
Describe how the data was lost?	

Reported by:	
Date:	

Send this report immediately to your

Club Chairperson

Annex C Investigation Template

1. Extent, nature and cause of the information loss:
   - Can this be determined, more or less immediately, with a high level of certainty?
   - Can this be determined within a number of days with a high level of certainty?
   - Can this not be determined with any level of certainty until much more detailed fact finding research is carried out?
   - Is this, apart from the general location of the business area, effectively unknown until the media 'go public'?
2. Immediate actions identified that can be taken to address system/ procedural vulnerabilities already highlighted as a result of the information loss.
3. Sensitivity of the information lost, or potentially lost, e.g. personal or sensitive data relating to customers or staff (informed by business area's Information Assets Register).
4. Is the potential extent of the information loss incident such that it requires setting up a response team?
5. Is the extent and nature of the information loss such that it requires more or less immediate notification to the data subjects and if so, will it need dedicated team/ special help-line?
6. Is there a need to escalate?

Annex D Follow-up assessment of data loss and relevant findings

Use this template to record relevant findings about the data loss incident

Description of the data which was lost or stolen:	Include the volume of records, whether or not it contains personal or sensitive personal data, the number of people affected.
Is the loss major?	See Risk Assessment Matrix at Annex D.
Explain your reasoning:	
How will the incident be handled?	Who will take overall control of the management of this issue. Normally it will be the Chairman who will undertake this role. Consider what decision making and administrative arrangements are needed. For example, a serious or major loss will need more resource; is a response team needed?
Who within the management committee has been informed or needs to be informed?	See Annex E for communication matrix which is based on severity of information loss.
Can the data be retrieved or reconstructed?	Include what actions can or have been taken. For example, if accidentally sent to the wrong person they should be asked to delete/destroy it without reading; if lost in a public place or stolen it may be necessary to report to the police.
Can or has further loss been prevented?	Include what actions can or have been taken. For example, issue a staff instruction; remove system access; lockdown web services; carry out a system audit.
Is it likely that the loss will cause harm to individuals?	If the answer is, “yes,” include an explanation of the potential harm and the likelihood of it happening.
Do data subjects need to be informed?	If the answer is yes, consider how they should be informed, e.g. individually by phone, fax, e-mail or letter. Consider if a press release or Club Newsletter would suffice.

Annex E Template Recovery Plan

Objective	Action	Responsibility	Progress / Date of completion

Annex F Template Event Log

Date	Time	Decision / Event / Action	Name