IT Security Policy

CONTENTS

Appendices

1. Introduction

The ease with which personal information can nowadays be passed within the Organisation- often by computer - is an undoubted benefit for employees and council members involved in the delivery of Ulster Badminton (UB) services. But all those concerned need to be aware that there is a legal duty to protect the confidentiality of employee, supplier and player information.

The public has the right to respect for their privacy, and hence an expectation that information about them will be treated as confidential. This IT Security Policy is based on that expectation, but also acknowledges that UB employees and council members will need to have strictly controlled access to employees, supplier and player information to ensure that UB functions effectively and efficiently.

In clarifying how and when personal information may be gathered and used, it confirms that a duty of confidence applies to everyone working for or with UB. This is emphasised by the fact that the General Data Protection Regulation (GDPR) includes **manual and computer** information.

1.1 Purpose of a Security Policy

Confidentiality data access is confined to those with specified authority to view the data

Integrity all system assets are operating correctly according to specification and in the way the current user believes them to be operating

Availability information is delivered to the right person, when it is needed

1.2 The Need for a Security Policy

The information stored on computers represents one of UB's most valuable assets. This information is at risk from many threats and there is therefor a need to implement measures which preserve its confidentiality, integrity and availability.

The purpose of this policy is to provide a range of IT Security defences against these threats, and also to ensure that, in so doing, UB is compliant with the prevailing legislation, including:

- the General Data Protection Regulation (GDPR)
- Computer Misuse Act 1990
- BS7799 Code of Practice for Information Systems Security

This policy relates to all IT systems operated by, and under the control of UB employees and members. (A list of which is enclosed in Appendix A.)

2. IT Security Policy Statements

2.1 UB has nominated their Administrator to have responsibility for the Council compliance with the General Data Protection Regulation (GDPR)

2.2 Each database that UB maintain will be updated by specified users and only specified users will have access to the database. These specified users will be responsible for ensuring that the UB gathers, holds and releases information in compliance with Legislation and Guidelines (Section 1.2).

2.3 Personal Computers will be the responsibility of each individual user.

2.4 UB will identify the actions required to implement and maintain the IT security measures outlined in this Policy, therefore this policy will be reviewed annually.

2.5 UB will implement effective mechanisms for regularly reviewing IT Security.

2.6 UB will monitor security breaches and imminent threats, and exchange information with external authorities if required.

2.7 Breaches of IT Security by employees may be considered to be a disciplinary matter.

3. UB Officers Responsibilities

3.1

- Ensuring that all IT systems in use are appropriately assessed for security compliance and are protected in accordance with the IT Security Policy.

- Ensuring that the UB IT security standards are implemented effectively and regularly reviewed.

- Monitor compliance with the GDPR, including the maintenance of the Councils Notification, and ensuring the adequacy of arrangements for the physical security of computers and contingency planning.

- Responsible for the receipt of all data requests for Subject Access under the GDPR; monitoring the procedures for fulfilling such requests, ensuring that the information supplied for the tracing of the data is sufficient, and ensuring the disclosure of the relevant information to the applicants within the specified time scale.

- Responsible for ensuring that UB employees, volunteers or service providers are kept aware of the requirements of the GDPR and their responsibilities under it. We will refer to 'Guide to the General Data Protection Regulation (GDPR)' as published by the Information Commissioner's Office on 25th May 2018.

- Receiving and considering reports of IT security incidents, initiating appropriate action and passing the reports to the UB Management Committee.

- Playing a proactive role in establishing and implementing IT security procedures and employees awareness.

- To monitor the effectiveness of IT security within UB and initiating any requested changes to security procedures which become necessary as a result of the monitoring process.

- Ensure that regular backups are taken and stored appropriately off-site.

- Ensure that appropriate levels of access are granted to system users.

- Ensure that all UB employees using the systems are aware of their IT Security responsibilities.

3.3 Users – Office Staff and Council Members

- Report IT Security incidents to the administrator and take action where appropriate.
- Comply with the UB IT Security Policy.
- Comply with Legislation and Guidelines in Section 1.2.
- Notify immediately the Administrator or the UB Management Committee of IT security breaches which come to their attention.
- Notify immediately the Administrator of any Data Protection breaches that come to their attention.

4. Security Measures

4.1 Virus Control

The deliberate introduction of malicious software to a system is a criminal offence under the Computer Misuse Act 1990.

4.1.1 No files should be loaded on to any system from an external source unless they have first been virus checked.

4.1.2 All servers, PCs and laptops will have anti-virus software installed.

4.1.3 Where a virus is detected this will be reported immediately to the Administrator who will arrange for a “clean” and rebuild. The affected PC will then be updated with anti-virus software.

4.2 Protection of Hardware from Theft

4.2.1 The UB Office is kept locked at all times. Access to the Office is restricted and access is only granted when required under supervision of a member of UB council or UB employees.

4.2.2 An asset register of computer equipment is maintained by UB employees under whose responsibility the equipment is placed.

4.2.3 No equipment should be removed from any site without the approval of the Administrator - except for portable computers that are the responsibility of each named individual user.

4.2.4 Hardware in particularly vulnerable areas or containing sensitive data should make use of physical security measures such as locking office doors or installing locking devices to secure hardware to desk.

4.3 Protection of Hardware from Accidental Damage

4.3.1 Care should be exercised when eating or drinking near IT equipment.

4.3.2 The location of all hardware (computers, printers, modems etc.) should comply with Health and Safety standards including the stability of the desk surface, and elimination of trailing cables.

4.3.3 All personal computers and printers should be switched off when not in use for extended periods, such as overnight or during weekends.

4.3.4 Air vents on computers should not be obstructed.

4.4 Protection of Data from Hardware Loss

4.4.1 Backups of data and system programmes will be taken on a regular basis.

4.4.2 Data should not be held locally on PCs alone; data should be saved to files on the servers.

4.3.1 Backup media will be stored securely off-site.

4.4.4 Backup recovery procedures will be tested on a regular basis.

4.5 Protection of Data from Unauthorised Access

4.5.1 Password controls must be implemented. Passwords should have the following

characteristics...

- Be at least 5 characters long
- Contain letters and numbers
- Be different from the previous passwords used
- Be user generated

4.5.2 System password details are recorded by individual users and kept securely.

4.5.3 Monitors used in public areas should be tilted away from the public's direct line of sight so that confidential information cannot be viewed.

4.5.4 Reports containing sensitive information (e.g. Payroll data) which require disposal should be shredded within the office shredder or placed within disposal bags for shredding as confidential waste.

4.5.5 Backups and copies of data should be stored securely off-site.

4.5.6 All storage media, including backups, should be clearly marked to avoid confusion over their contents.

4.5.9.1 Where appropriate, physical controls should be used to prevent unauthorised access.

5. Protection of Personal Data

In addition to the GDPR data protection principles (Appendix B), which UB will undertake to abide by, there are also several key points which stress: -

5.1 The Public have a right for their privacy to be respected and hence an expectation that information about them will be treated as confidential.

5.2 All UB employees have a common law duty of care to protect personal information.

5.3 UB must have an active policy for informing data subjects of the kind of purposes for which information about them is collected.

5.4 Arrangements (both manual and technology based) for the storage, disposal and handling of information must protect confidentiality. Care should be taken to ensure that unintentional breaches of confidence do not occur.

5.5 Breach of confidentiality is a serious matter that may result in disciplinary action by UB or legal action by a player or supplier.

5.6 All data requests must be forwarded to the UB Administrator.

6. Protection of Connection to Other Networks

6.1 The LAN (Local Area Network) will not connect to any other network unless UB is able to control access from outside users into the LRC network.

6.2 UB will utilise Firewall protection to prevent illegal intrusion via the internet.

7. Software Control

7.1 All software purchases must be agreed by the UB Council and no software (including evaluation software) should be installed without permission from UB.

7.2 Software must not be copied, as this is an infringement of copyright and therefore illegal - unless specifically permitted by the licensing agreement. This includes loading the software from one set of disks onto several PC's.

7.3 All System Software disks will be stored securely in the Ulster Badminton Office Store. These are the only proof of a legal license to use the software, and may be required to be produced in evidence should the Federation Against Software Theft (FAST) investigate.

8. Reporting of IT Security Breaches

8.1 Any employee or UB Council member, can report a violation (or a suspected violation) of the above practices to the Administrator. The Administrator will then assess the level of risk associated with the violation and take appropriate action to minimise the risk and prevent re-occurrence of the violation.

9. Special Considerations for the use of Portable Computers

All previous policy statements apply to portable computers and the following special considerations as by their nature, portable computers are the most vulnerable to theft or loss.

9.1 Portable computers should not be left unattended i.e.. in a car, hotel room, office or even at home.

9.2 Backups should be taken and stored securely of all sensitive information.

9.3 Passwords should be used on sensitive information wherever possible.

9.4 Laptop theft is the most common security breach – if confidential data is going to be stored on a laptop it must be adequately protected using a password.

10. Special Considerations for use of the Internet and Electronic Mail

10.1 The UB (LRC-Badminton) Local Area Network will not be connected to the Internet using any protocol which may allow Internet users onto the LAN.

10.2 No personal computer that is attached to the UB (LRC-Badminton) Local Area Network shall connect to the Internet using any protocol that may allow Internet users to enter the Council LAN.

11. Using the Internet

This is detailed in UB 's Internet Policy - Appendix D

Acceptable Use

11.1 Use of the Internet by employees or council members that can be deemed to be of an illegal, offensive or unethical nature is unacceptable and therefore just cause for taking disciplinary action e.g.

- Violation of copyright, license agreements or other contracts for example copying and using software for business purposes from a site where there is a clear limitation for personal use only;

- Downloading or viewing any information which could be considered illegal or offensive e.g. pornographic or racist material;

- Successful or unsuccessful attempts to gain unauthorised access to information resources - commonly known as 'hacking';

- Using or knowingly allowing someone else to use any computer, computer network, computer system, program or software to devise or execute any artifice or scheme to defraud or to obtain money, property, services, or other things of value by false pretences, promises or representations;

- Without authorisation destroying, altering, dismantling, disfiguring, preventing rightful access to or otherwise interfering with the availability and/or integrity of computer-based information and/or information resources;

- Without authorisation invading the privacy of individuals or entities that are creators, authors, users or subjects of the information resources; for example reading the e-mail of another without permission;

- Using the Internet for political lobbying;

- Transmitting or causing to be transmitted, communications that may be construed as harassment or disparagement of others; and

- Violating any UK laws pertaining to the unauthorised use of computing resources or networks.

11.2 Personal use of the Internet should only be during employees free time and should always take second place to the carrying out of work duties.

It is not acceptable for resources and, in particular, employees time to be wasted in casual surfing/browsing of the Internet. However, personal use is permitted provided all guidelines within this document are adhered to, accesses are minimised and are of a specific nature (as opposed to casual and aimless browsing), i.e. directed to a specific Web page or a particular subject matter.

11.3 Employees should not log on to the Internet and remain continuously connected throughout the day.

Employees interested in sport or the money market, for example, may be tempted to log on to the relevant Internet service to receive continuous updates. This practice unfairly uses up scarce 'bandwidth' and will slow down response times for other legitimate users.

11.4 UB employees can order goods or services for personal use, during employees' free time.

Particular attention is drawn to those Web pages in which there are response forms and/or mail back facilities. For example some Web pages present opportunities to form contracts specifically in relation to purchasing of goods or services.

11.5 Downloading of Files & Software

No file should be downloaded from or via the Internet unless it is in connection with the user's job.

Particular attention must be paid to any specified licensing specifications or other similar conditions. Employees are not permitted to enter into any agreement on behalf of UB.

Where permission to download is not explicit to do so, could be deemed to be 'hacking' or in breach of copyright laws and expose UB to civil and criminal liabilities should also avoid downloading large files (> 1 Mb).

12. Use of E-Mail

12.1 Introduction

Increasingly e-mail is being seen as the preferred mechanism for communicating not only internally within an organisation but also externally to other organisations outside UB. While it would be foolish to ignore the obvious advantages to all parties in using this technology, particularly in view of the fact that others external to this organisation initiate many contacts using this method, employees must accept the need to be professional in approach whenever communicating externally, irrespective of the medium.

Unlike other forms of communication there are also special security issues with e-mail including the inadvertent introduction of computer viruses and the danger of messages being read by other than the intended recipient. This is particularly so for e-mail that may be sent or received via less secure networks such as the Internet.

All employees must follow the policy as stated in Appendix D. It applies to any electronic mail whether internal or issued to or received from, external sources and it applies equally to Internet mail as well as normal e-mail facilities.

The actual policy statements are contained in Appendix D to this document however the paragraphs below explain the reasoning behind the policy to enable employees to have a clear understanding of the need for such rules and guidelines.

12.2 Outgoing Email - Tone And Content

Writing a letter and having it typed on headed notepaper almost automatically instils a 'formality of tone' on the author, and this is a good thing (but not forgetting the spirit of the 'Plain English' campaign). However, e-mail almost has the exact opposite effect. Tone and content tend to be much more relaxed and humour can be the norm and this is not necessarily a good thing when dealing with outsiders. **Email is not a written telephone conversation.** It is difficult to put a laugh into your words even if you were smiling when you wrote them!

Care too needs to be taken when responding to an e-mail. The tone of response is often dictated by the tone of the originating message, nevertheless, without being bureaucratic or stilted or needlessly formal, frivolous e-mail should be avoided even where the original message may itself appear to be frivolous.

Email being sent externally, and even e-mail being sent to another department within this organisation, that is dealing with business matters, i.e. not messages confirming the date and time of a meeting for example, should not be treated any less formally than more traditional paper-based methods of communication and, if appropriate, should be approved before dispatch in the same way as a draft letter may require approval. Clear and succinct language should be used and the same standard of grammar and spelling should be applied in the same way that they would be applied to letters on headed stationery. Obviously it is not necessary to begin with 'Dear ...' or finish with 'Yours sincerely ....'.

'Business' messages should be printed and filed in the same way as formal letters. It may even be appropriate to check the Receipt box and print off and file the resulting return message if the original message is of particular importance and a record of receipt is thought desirable.

12.3 Outgoing E-Mail - Attachments

It is often seen as more convenient to attach a document to an e-mail message than it is to send a copy with its accompanying letter by ordinary mail. This might be true for the sender but it is not always so for the recipient and may even be problematic in respect of the network and security in general.

Consider the Recipient

A document viewed by the sender using his or her own word processor or spreadsheet software may look to be in perfect order on screen and when printed. However, the recipient may be unable to read the document at all because he does not have the same software; his version is lower than that used to create the document; or his software is otherwise incompatible. Even where a recipient's software is able to 'import' documents created by something else there may be formatting difficulties sometimes to the extent that extensive reworking is required on receipt to make the document readable.

12.4 Outgoing E-Mail - Security

The route by which e-mail is delivered is often circuitous and may even involve being exposed to very insecure networks. Users should remember that e-mail messages can be intercepted due to the nature of the internet. It is possible to set up routines that can scan passing e-mail for key words without being detected - the Internet equivalent of phone tapping. Consequently, employees should give very serious consideration to the contents of any message or attachments sent by e-mail.

The content of e-mail is subject to all applicable UK laws such as those relating to copyright, defamation, data protection and public records, as well as statutes concerning the sensitive and contentious issue of pornography. Obviously nothing illegal or infringing a third party's intellectual property rights should be included in an email.

12.5 Outgoing E-Mail - Private Use

Management is aware that employees often make use of e-mail for private reasons, contacting relatives in foreign parts for example. Personal use of e-mail is permitted provided such use is only during free time and is not of significant volume. Particular attention is drawn to the above paragraph on security.

12.6 Incoming E-Mail

Know whom you are talking to. Although this may seem to be an obvious thing to do employees should always read who sent the message before reading, and perhaps reacting to, the message itself.

12.7.1 Checking for Viruses

The main text of an e-mail message **cannot** contain a virus.

Any attachments to an e-mail message **can** contain a virus and employees must take care when dealing with these. Provided all PCs within the Ulster Badminton Office contain anti-virus software employees can assume that any attachments to email messages originating internally are virus-free. However, there is no guarantee that attachments to mail received from outside the Ulster Badminton Office are similarly safe. Remember that the developers and suppliers of anti-virus software are of course, always at least one step behind the creators and distributors of viruses.

Employees should note that while the automatic anti-virus software is able to detect and can subsequently delete viruses, through either "cleaning" the attachment or removing the attachment altogether. Users should be aware that attachments containing viruses can damage not only the host PC but potentially also the server. This will result in disruption to the work of the PC's 'owner' and create additional and avoidable work for IT Services.

A particularly dangerous type of virus is that known as a Trojan horse. These can arrive as e-mail attachments and, indeed, are often attached to e-mail claiming to enhance security. Typical actions by this type of virus include the deletion of files on the hard disc but, some can locate the user's password, and anything else, by following keystrokes - a technique known as 'sniffing'. The sniffed data is then sent back to the hacker via e-mail.

While there is defence against these Trojan horses' employees can at least take steps to reduce the likelihood of introducing viruses of any description by following the procedures contained in the policy.

Particular attention should be given to attachments from unknown or dubious sources. Where there is doubt or suspicion, advice should be sought <u>before</u> any such attachment is opened.

12.7.2 Reporting Viruses

The virus scanning software will automatically notify the user of any virus discovered in an attachment.

However, sometimes mail messages themselves (not to be confused with the attachments) claim to warn of viruses. There have been some cases, although not always, in which such

warnings have been hoaxes that nevertheless waste time and effort and cause unnecessary panic if passed on to others. Employees must, therefore make the Administrator aware of such warnings and not to any others, either internal or external to the Ulster Badminton Office.

IT Security Policy

APPENDIX A

MAIN ULSTER BADMINTON OFFICE IT SYSTEMS

MS Windows 10	Operating System
MS Outlook 2010	Mail & Diary system
Microsoft Office 2010	Office Productivity Software

APPENDIX B

ARTICLE 5 OF THE GENERAL DATA PROTECTION REGULATION

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

A: processed lawfully, fairly and in a transparent manner in relation to individuals;

B: collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

C: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

D: accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

E: kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

F: 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.

When handling Personal Data, employees must be aware of, and adhere to, these principles particularly with regard to passing data on to other users**.**

APPENDIX C

IMPORTANT DO'S AND DON'TS

DO

- Save all documents to appropriate server
- Store your backups and system disks securely off site
- Change your confidential passwords regularly
- Report Information Technology Security Breaches to the Administrator

DON'T

- Leave your PC switched on overnight or unattended for long periods of time
- Save files locally on PC hard drive
- Load software – any software requirements must be coordinated by the Administrator.
- Remove hardware without notification of the Administrator.
- Use Personal Data unless you are sure that it is in compliance with the GDPR

APPENDIX D

USE OF E-MAIL - THE POLICY

1. The E-Mail system must not be used to:

   - transmit obscene, offensive or damaging material;
   - transmit threatening material or material intended to frighten or harass;
   - transmit defamatory material;
   - infringe copyright;
   - transmit unsolicited advertising or similar activities;
   - attempt unauthorised access to other networks or systems.

2. Employees should restrict the recipients of e-mail messages to those who actually may have interest in the message contents. The occasional general interest message or query to all for example is permitted but on-going e-mail conversations, which may be of little interest to many of the recipients, should be restricted.

3. Employees should check e-mail inboxes at least daily and provide responses appropriate to the importance of the message.

4. In order to ensure an efficient service unwanted messages should be deleted.

5. Employees have the ability to protect their own e-mail account through the use of passwords and should use this facility using passwords not easily detectable. Employees will be held accountable for all e-mails originating from their own account; therefore password protection is of utmost importance.

6. Unauthorised access to other users' e-mail accounts is prohibited.

7. E-mail messages must be clear and concise and, for external messages, tone and content must be suitable for a business communication and appropriate to the medium.

8. Formal communications i.e. where otherwise a UB headed letter may have been used, should be printed and filed, along with any attachments, in the appropriate Registered File.

9. No passwords of any description may be transmitted via e-mail.

10. In order to ensure appropriate corrective action is taken, and no unnecessary panic is caused by hoaxes, employees must report any virus incidents immediately or any other apparent breach in security. Employees must not take it upon themselves to issue warnings to employees within or outside the Ulster Badminton Office.

11. Personal use of E-mail is permitted provided the above rules and guidelines are followed; such personal use is restricted to employees' free time and is kept to reasonable levels. Employees are also instructed to include the disclaimer below in all personal e-mail:

    "*This e-mail is a personal communication and is not authorised by or sent on behalf of any other person or UB"*

    Abuse of this privilege will result in its withdrawal and possible disciplinary action against the employees concerned.

12. Failure to comply with this policy may result in disciplinary action.

APPENDIX E

IT SECURITY POLICY AGREEMENT

To: ULSTER BADMINTON

From:

I hereby acknowledge receipt of Ulster Badmintons rules relating to IT Security.

I understand that **all employees and council members must adhere to these rules**, and that any breach will be dealt with under Ulster Badmintons Disciplinary Procedure(s).

Signed: _____ Date: _____