The Wallingford Sports Trust
Policies and procedures

16. Information Technology Policy

Contents

Version: 1
Date: 03 Dec. 2018

The Wallingford Sports Trust
Policies and procedures

Information Technology Policy

This Policy document is guidance for The Wallingford Sports Trust's ("The Trust") employees, trustees and volunteers on the behaviour and use of technology that is approved by the Trust. This document will be reviewed and updated by the trustees on an annual basis or when relevant to include newly developed security standards into the policy.

This policy will help the Trust ensure that it:

- Minimises financial and reputational risks from breaches of confidential, copyright, personal data or commercially sensitive information.
- Avoids bullying, harassment or embarrassment to employees or the Trust.
- Minimises disruption to our activities; and
- Complies with applicable laws.

1. Protecting our equipment and data

When using Trust devices (including desktop devices and smartphones) employees should always ensure they are:

- Up to date with anti-virus software
- Up to date with any latest software updates
- Secured with strong passwords.
- Returned when an employee leaves the employment of the Trust.
- Never left unsecured in an unlocked office.

2. Use of personal devices

This refers to the use of personal devices by the Trust's employees or trustees to store or access Trust data. This includes desktop computers, laptops, tablets, smartphones or other specialise digital equipment.

Users of personal devices to store or access Trust data must ensure that they are:

- Up to date with anti-virus software
- Up to date with any latest software updates
- Secured with strong password or pass codes.
- Set up with an auto lock (device locks automatically after an idle time period)
- Aware when connected to untrusted or unsecured WiFi networks which could open up unauthorised access to Trust data.

The Trust takes no responsibility for the maintenance support or costs associated with personally owned devices.

The Wallingford Sports Trust
Policies and procedures

3. Collecting and storing data

When collecting or storing Trust data, Trust employees and trustees should always:

- Limit the amount of personal data which is collected.
- Where possible keep Trust data separate from any personal information.
- Ensure all key information and data is backed or stored on the Trust dropbox.
- Limit the number of copies in circulation. If copies of data are stored on many different devices, say as an attachment in an email, there is an increased risk that personal data will become out-of-date or inaccurate over time. There is also an increased risk that it will be retained for longer than is necessary, due to the fact that it is more difficult to keep track of all copies of the data. Therefore where possible data should be stored in the WST dropbox to ensure a single source.

4. Sharing data

When sharing information users should:

- Always use a secure means of transfer.
- Minimise the quantity and extend of data which is shared outside the Trust.
- Encrypt or password protect any files which contain any personal or sensitive information.
- On removable media such as USB memory stick, CD ROMS etc, take care not to misplace or leave unsecure.
- Ensure that the email address being used is the correct or appropriate one.

5. Disposal of Stored Data

All data must be securely disposed of in accordance with the Trust Retention Policy when no longer required by the Trust, regardless of the media or application type on which it is stored.

6. Internet Use

The internet is a powerful tool that can bring significant benefits to the Trust. For example employees, Trustees and volunteers may use the internet to purchase office supplies or update the website or media sites. It is therefore important that users understand how to use it responsibly, safely and legally. This applies to use of the internet on any device that is owned by the Trust, or that is connected to any of the Trust's networks or systems .For example, it applies both to an employee using the internet at their desk, and to employees, trustees or volunteers who connect their own tablets or smart phones to the Sports Park wireless network.

The Wallingford Sports Trust
Policies and procedures

Internet Security

Used unwisely, the internet can be a source of security problems that can do significant damage to the Trust's data and reputation.

- Users must not knowingly introduce any form of computer virus, Trojan, spyware or other malware into the Trust.
- Employees and other users must not gain access to websites or systems for which they do not have authorisation, either within the Sports Park or outside it.
- Trust data should only be uploaded to and shared via approved services.
- Employees or other users must not steal, use, or disclose someone else's login or password without authorisation.

Employees and other users must always consider the security of the Trust systems and data when using the internet.

Inappropriate Content and Uses

There are many sources of inappropriate content and materials available online. It is important for employees and other users to understand that viewing or distributing inappropriate content is not acceptable under any circumstances. Users must not:

- Take part in any activities on the internet that could bring the Trust into disrepute.
- Create or transmit material that might be defamatory or incur liability for the Trust.
- View, download, create or distribute any inappropriate content or material. Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs. This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
- Use the internet for any illegal or criminal activities.
- Send offensive or harassing material to others.
- Broadcast unsolicited personal views on social, political, religious or other non-business related matters.
- Send or post messages or material that could damage the Trust's image or reputation.
- Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.
- Download illegal copies of music, films, games or other software, whether via file sharing services or other technologies.

The Trust's information technology and internet resources — including computers and internet connections — are provided for legitimate business use.

Version: 1
Date: 03 Dec. 2018

The Trust therefore reserves the right to monitor use of the internet, to examine systems and review the data stored in those systems. Any such examinations or monitoring will only be carried out by authorised persons. Additionally, all internet data written, sent or received through the Trust's computer systems are part of official Trust records. The Trust can be legally compelled to show that information to law enforcement agencies or other parties.

7. Email

The Trust recognises that email is a key communication tool and it encourages employees, trustees and volunteers to use email whenever appropriate.
Although a relatively informal medium, users should be aware that each email they send does affect the Trust's image and reputation. Users should always ensure that the business information sent via email is accurate, appropriate, ethical and legal.
Users must be careful about making commitments or agreeing to purchases via email as an email message may form a legally binding contract between the Trust and the recipient – even if the user has not obtained proper authorisation from the Trust.

Email security

Used inappropriately, email can be a source of security problems for the Trust. Users of the Trust email system must not:

- Open email attachments from unknown sources, in case they contain a virus, Trojan, spyware or other malware.
- Disable security or email scanning software.
- Access another user's Trust email account.

Users should note that email is not inherently secure. Most emails transmitted over the internet are sent in plain text. This means they are vulnerable to interception. Although such interceptions are rare, it's best to regard email as an open communication system, not suitable for confidential messages and information.

Inappropriate email content and use

The Trust's email system must not be used to send or store inappropriate content or materials. It is important users understand that viewing or distributing inappropriate content via email is not acceptable under any circumstance.
Users must not:

- Write or send emails that might be defamatory or incur liability for the Trust.
- Create or distribute any inappropriate content or material via email. Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs. This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or

political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

- Use email for any illegal or criminal activities.
- Send offensive or harassing emails to others.
- Send messages or material that could damage the Trust image or reputation.
- Use the Trust's email system to perform any tasks that may involve breach of copyright law.
- Send bulk emails for marketing purposes.

Any user who receives an email they consider to be inappropriate should report it to one of the Board of Trustees.

The Trust's email system is provided for legitimate business use and the Trust therefore reserves the right to monitor employee use of email. All emails sent or received through the Trust's email system are part of its official records and the Trust may be legally compelled to show that information to law enforcement agencies or other parties.

8. Social Media

The Trust recognises that Social media can bring significant benefits to the Trust, and offers a platform for the Trust to perform marketing, stay connected with customers and club members and build its profile online.

However, it is important that users who use social media within the Trust do so in a way that enhances the Trust's image .A misjudged status update can generate complaints or damage the Trust's reputation. There are also security and data protection issues to consider.

Social media sites and services include (but are not limited to):

- Popular social networks like Twitter and Facebook
- Photographic social networks like Flickr and Instagram
- Professional social networks like LinkedIn

To ensure the Trust's social media presence is consistent and cohesive, only people who have been authorised to use the Trust's social networking accounts may do so. Authorisation is usually provided by the Board of Trustees.

New social media accounts in the Trust's name must not be created unless approved by the Board of Trustees.

Purpose and Use of Trust's social media accounts

In general users should only post updates, messages or otherwise use these accounts when that use is clearly in line with the Trust's overall objectives.

For instance, users may use the Trust's social media accounts to:

- Respond to customer enquiries and request for help
- Share blog posts, articles and other content created by the Trust
- Share insightful articles, videos, media and other content relevant to the Trust but created by others.
- Provide Club members or followers with an insight into what is going on at the Trust.
- Promote marketing campaigns and special offers.
- Support new product launches and other initiatives

Safe,responsible social media use

The Trust's social media accounts must not be used to share or spread inappropriate content or to take part in any activities that could bring the company into disrepute.

When sharing an interesting blog post, article or piece of content, users should always review the content thoroughly and should not post a link based solely on a headline.

Security and data protection

Users should be aware of the security and data protection issues that can arise from using social network. Users must:

- Maintain confidentiality and not share content or information which could be commercial sensitive.
- Protect social accounts using strong passwords.
- Avoid scams by watching for phishing attempts

The Trust will monitor the use of social networks.

9. Breach of Policy

Knowingly breaching this policy is a serious matter. Employees who do so will be subject to disciplinary action, up to and including termination of employment. Any breach by 'other users' will be referred to the Board of Trustees to determine what course of action should be taken against the individual(s) concerned.

Employees and other users may also be held personally liable for violating this policy.

Where appropriate, the Trust will involve the police or other law enforcement agencies in relation to breaches of this policy.