PLYMOUTH ARENA

IT POLICY

VERSION: 2.0

DATE: 06/11/2025

REFERENCE NUMBER: PA/IND08/2025/ITP

RESPONSIBLE PERSON: RICHARD FINDLAY

DATE FOR RENEWAL: NLT 5 YEARS

ICONIC.
INDEPENDENT.
YOURS.

IT POLICY

PURPOSE

The purpose of the IT policy is to ensure the effective protection and proper usage of the computer systems at Plymouth Arena. Adhering to this IT policy will assist in assuring the systems continue to operate efficiently and effectively. Contraventions of the IT policy could seriously disrupt the operation of the business and any breaches will be treated seriously.

SCOPE

This policy applies to all staff that have computer access and work at Plymouth Arena.

POLICY

This IT Policy is central to the way we operate and as such the overall responsibility for its implementation rests with the Chief Executive and the Senior Management Team.

The Chief Executive and Senior Management Team will, through the delivery and implementation of this policy and associated tools, ensure that all managers receive appropriate instruction to support their understanding of the IT Policy and enable them to consistently apply the principles therein.

Managers, Coordinators and Supervisors have specific responsibilities to ensure that their individual teams read and follow this policy and keep up to date with current legislation and best practice.

The Chief Executive and Senior Management Team will:

- Endorse and support the policy
- Ensure all line managers are made aware of the policy and their responsibilities within it
- Undertake that the policy shall be reviewed annually and amended as necessary to reflect legislative or best practice changes
- Ensure staff are aware of the data protection regulation (GDPR) and trained accordingly

AVAILABILITY OF THE POLICY

A copy of this policy is available to all current employees:

- As part of their staff induction
- Accessible here: I:\global policies & procedures\GDPR

PROTECTION OF IT EQUIPMENT, SYSTEMS & INFORMATION

Network management, administration and maintenance within Plymouth Arena is the responsibility of the external IT management company called The ITEC Group. Access to and usage of the servers is restricted to ITEC and the Senior Management Team. Attempts to access information or systems without the necessary system approval put in place by ITEC may be considered a disciplinary offence and will result in disciplinary action. Deliberate damage or misuse of electronic files, systems, hardware, network or internet will result in disciplinary action. The installation, configuration and maintenance of networked computer equipment is the responsibility of The ITEC Group. Any purchase of computer equipment, systems and

software must be approved by Senior Management. All electronic information generated and stored at Plymouth Arena and the Box Office, is the property of Plymouth Arena. With the exception of departmental IT equipment (such as the Tech department for show purposes); the relocation of any computers, printers (including Toner and Drum), other peripherals and any network connections must only be undertaken by the ITEC Group or an in house trained person. All problems with hardware & software should be reported to the relevant line manager and the ITEC Group as soon as possible. Details on how to raise a support request are detailed below under *Procedures*.

REMOTE WORKING

Security measures must be obeyed at all times regardless of the location of work. Where your job role specifies; the company may permit you to work remotely, or from home. In such cases, you may be supplied with a company laptop or other mobile device, which allows you to access e-mails and the company network to complete work tasks for commercial purposes. Employees using portable IT equipment away from the premises belonging either to Plymouth Arena, or be authorised to use their own personal devices; must take all reasonable care to ensure all items remain safe and any data remain secure, and in compliance with the General Data Protection Regulation (GDPR) 2016/679. Access to the company's documentation and network must only be available via secure VPN through the companies IT provider ITEC, and not through any portable device such as USB. Any loss of IT equipment, or incident where company information and personal data may have been compromised and therefore presenting a data breach - must be reported immediately to the Data Response Team.

SOFTWARE

All software, including anti-virus protection, must have an original license and be installed by The ITEC Group using genuine media. Requirements for new software/software applications should be discussed in advance with an employee's line manager and in some cases the senior management team, to allow detailed assessment of specification and any possible implication to the business. Software including games, MSN, screensavers, programs from the Internet etc, must not be installed on the system.

USER ACCOUNTS AND PASSWORDS

Line managers should notify The ITEC Group in advance, via a support request, of joiners and leavers to allow the creation/deletion of user accounts. Employees are responsible for the security of their passwords and accounts which should not be shared with, or disclosed to any other party. It is recommended that individual passwords are alphanumeric, eg. Se123£, with a minimum of 6 characters. For security purposes passwords will be required to be changed when prompted by the system. Passwords may be reset in an emergency with the approval of ITEC and the individual user will be informed. Apart from specific machines labelled accordingly, users should ensure their computers and monitors are fully shut down and turned off at the end of the day, or when likely to be left for a period of time. To protect the individual and maintain network security, users are to log off or lock their computers when leaving their work area. Department managers will determine the associated permissions and security status of folders/directories for their department.

EMAIL

The e-mail system is a core business application. It must not be used for political, business or commercial purposes unrelated to Plymouth Arena. The Plymouth Arena e-mail system must not be used to send illegal or inappropriate material. All e-mails generated or received through the company e-mail system are the

property of Plymouth Arena. Personal use of e-mail is not permitted unless approved by an employee's line manager. If granted employees should ensure there is no abuse of this privilege. Global distribution lists should be used for Plymouth Arena business purposes only.

EMAIL GUIDELINES AND INFORMATION

Personal opinion is open to interpretation; employees should always write in a professional capacity as representatives of Plymouth Arena. E-mails may be used as evidence in a court of law, so opinion should be carefully thought out before being committed to 'paper'. Attachments should be restricted in size where possible. Advice on sending larger attachments can be sought from The ITEC Group.
E-mail can always be traced back to source if and when required.

INTERNET GUIDELINES

An employee's historical Internet usage may be viewed upon the approval of a Senior Manager. The company internet or network may not be used for private trading or commerce not associated with the business of Plymouth Arena. Access to the Internet is provided for business relating to Plymouth Arena. Limited personal use is permitted with line manager approval however, employees should ensure there is no abuse of this privilege. The Plymouth Arena system must not be used to access pornographic, illegal or other improper material. Staff must not subscribe to chat rooms, dating agencies, instant messaging services or other online subscription Internet sites unless they pertain to work duties or have approval from a line manager. Abuse of Internet access will be dealt with through the company disciplinary policy.

SOCIAL MEDIA

The use of personal social media accounts at work is prohibited, unless approval has been given by the employee's line manager and/or the Senior Management Team. Plymouth Arena marketing team have access to the company social media accounts for business purposes. The company social media accounts may be linked via members of the marketing team's personal accounts for 'admin privileges'. The Plymouth Arena marketing team follow strict guidelines regarding posting and changing any online content. Guidelines for this can be found in the Marketing Normal Operating Procedures and the Marketing Branding Guidelines.

All employees of Plymouth Arena are expected to portray both companies in a professional light at all times. This includes when using their own personal social media accounts.

Employees could face disciplinary proceedings for social media content that impacts on their reputation and the reputation of the company, as well as any comments about others which are derogatory or discriminatory or which amount to bullying or harassment, whether such comments are posted during working time or in their own time.

Employees should remember the following:

- The organisation has a dedicated team tasked with responding to customer enquiries or criticism. Our official Plymouth Arena marketing team is responsible for engaging customers through our various social media channels. To avoid confusion, we ask employees not to respond to customer enquiries or comments directed specifically to the company, or that ask for an official company response.
- For job specific issues; while we encourage employees to join our social media channels, we encourage employees to direct any complaints or concerns about their job or working environment

directly to their line manager using the established reporting processes as detailed in the Grievance or the Inappropriate Behaviour policy in the 'How to make a complaint' section.

- Employees should not comment on any topic relating to legal matters, litigation or any parties the company may be in litigation with.
- Employees should not participate in social media when the topic being considered is a crisis situation. Please refer all social media activity around crisis topics to the marketing department.
- Employees should not create company specific social media profiles.

Note: The above does not apply to employee's personal use of social media platforms outside of work-hours where the employee makes no reference to company related topics.

GDPR

The General Data Protection Regulation (GDPR) 2016/679 is a regulation in law on data protection and privacy for all individuals. It also addresses the export of personal data. All employees with computer access that work for Plymouth Arena are required to complete a GDPR knowledge test when they start their employment. This will be kept on record within their personnel files.

For further information regarding GDPR, please refer to the company GDPR policy accessible here: I:\global policies & procedures\GDPR

ENFORCEMENT

MANAGERS, COORDINATORS AND SUPERVISORS

Managers, Coordinators and Supervisors have a responsibility to ensure that their staff members and relevant teams have the correct system permissions in order to carry out their specific duties.

Managers and Coordinators are also responsible for communicating this policy and ensuring compliance with it within their areas of responsibility.

INDIVIDUAL EMPLOYEE RESPONSIBILITY

An employee's responsibilities are to ensure that they:

- Follow this IT policy at all times
- Report any IT problems to their line manager and ITEC without any reasonable delay.
- Do not miss-use or abuse the company computer system and/or the internet.

- Portray the company in a positive light at all times
- Return any assets upon termination of contract

PROCEDURE

If an employee requires any changes to their login, software or part of the computer system, a ticket request is to be created and sent to the external IT management company ITEC. The email address to send a request to is: support@itecgroup.co.uk and the phone number to call is: 0117 951 1500. Certain support requests may require Senior Management approval, e.g. creating new logins, adding software and gaining access to system drives. Once a support request has been raised (also known as a ticket)

the employee that sent the original request will receive a receipt email containing a ticket number. For a password reset an employee is required to contact ITEC on the number above.

ADDITIONAL INFORMATION

For additional information please see the below links:

1990 computer misuse act - https://www.legislation.gov.uk/ukpga/1990/18/contents

Use of display equipment at work - http://www.hse.gov.uk/msd/dse/

GDPR 2016/679 information - https://www.local.gov.uk/our-support/general-data-protection-regulation-gdpr

ITEC group support website - https://www.itecgroup.co.uk/get-support/