



IT Security policy

PORTSMOUTH COMMUNITY FOOTBALL PFC

Version 1.1

February 2024

Prepared by

Name	Department/Role	Date
Darren Parker	Head of IT systems	08/11/2022

Reviewed by

(this policy is under periodic review and PORTSMOUTH COMMUNITY FOOTBALL PFC reserves the right to update or amended it at any time. Any amendments made will be notified to members of staff).

Name	Department/Role	Date
Darren Parker	Head of IT systems	10/02/2023

Approved by

Name	Department/Role	Date
Darren Parker	Head of IT systems	10/02/2023

Revisions

Name	Change	Date	Version
Darren Parker	Addition of BYOD wording	20/01/2024	V1.1

Contents

Purpose and Context.....	5
Scope.....	5
1. Introduction	5
1.1. The threats we face.....	5
1.2. IT Security Procedure Manual.....	6
2. Compliance.....	6
3. Information Handling	6
3.2. Precautions against hardware, software, or data loss	6
3.3. Disposal of equipment	7
3.4. Working practices	7
3.5. Off-site removal and cloud storage of data.....	7
3.6. Backup and recovery	7
3.7. Archiving	8
3.8. Information lifecycle management	8
3.9. Sensitive or confidential information.....	8
3.10. Use of electronic communication systems	8
3.11. Additional data protection declaration requirement.....	9
4. Mobile and Remote Computing.....	9
4.1. Authorisation	9
4.2. Use of computing equipment off-site	9
4.3. Travelling	10
5. Outsourcing and Third Party Access	10
5.1. External suppliers.....	10
5.2. Security and confidentiality verification	10
5.3. Service level agreements	11
6. Operations.....	11
6.1. Building access control.....	11
6.2. Operational procedures	11
6.3. Procedure for reporting of concerns.....	11
6.4. Change management	11
6.5. Risk assessment	12
6.6. Security Testing	12
7. User Management	12
7.1. User identification.....	12
7.2. ID security	12

7.3. Access control standards.....	12
7.4. Starters, Leavers and Affiliates	13
7.5. User training.....	13
8. System Planning	13
8.1. Authorisation	13
8.2. Secure Configuration and System Hardening.....	13
8.3. Risk assessment and management	13
8.4. Access control	14
8.5. Testing	14
9. IT Systems Management	14
9.1. Staffing	14
9.2. Access control	14
9.3. Privileged Access Accounts	15
9.4. Change management	15
9.5. Network design	15
9.6. Logging	16
9.7. System Patching.....	16
9.8. Device Management	16

Purpose and Context

The purpose of the IT Security Policy is to ensure business continuity and to minimise operational damage by reducing the opportunity for and impact of security incidents.

Scope

This Policy applies to all IT-related systems, hardware, services, facilities and processes owned or otherwise made available by the Portsmouth Football Club “PFC” or on its behalf, whether utilising the PFC’s network and servers or those provided through cloud-based environments. This policy includes, for the avoidance of doubt any personally owned devices that are used in connection with PFC activities (together, **IT Systems**). This policy applies to all users and administrators of IT Systems, inclusive of PFC staff, contractors, affiliates, and third-party providers.

1. Introduction

1.1. The threats we face

PFC is facing increasing security threats from a wide range of sources. Systems and networks may be the target of a variety of attacks, including computer-based fraud, data theft, surveillance or vandalism. Such threats to IT security are generally expected to become more widespread, more ambitious and increasingly sophisticated.

Because of increasing dependence on IT systems and services, PFC is becoming more vulnerable to security threats. The growth of networking, cloud services and mobile devices presents new opportunities for unauthorised access to computer systems or data and reduces the scope for central, specialised control of IT facilities.

In addition, legislation exists which places legal requirements on PFC to protect personal privacy and to ensure the confidentiality and security of information and that its use is within the law. This legislation includes the Data Protection Act 2018, the Copyright, Designs and Patent Act 1988, The Regulation of Investigatory Powers Act (RIPA) 2000, the Computer Misuse Act 1990 and the Counter-Terrorism and Security Act 2015 (which encompasses the ‘Prevent’ duty).

This Policy contains terms relating to the classification of data. There are three classifications: sensitive, confidential and general. Direction on which types of information fall into the different categories is set out in the IT Security Procedure Manual (see below).

This Policy should be read in conjunction with the following PFC documents:

- Data Protection Policy
- Retention and Disposal Schedule
- Using your own device Policy

1.2. IT Security Procedure Manual

This Policy is supported by the IT Security Procedure Manual, which contains detailed guidance and operational procedures to help to ensure that users and administrators of PFC's IT systems do so in compliance with this Policy.

2. Compliance

PFC's Regulations Governing the Use of IT services set out the responsibilities of anyone using PFC IT Systems.

3. Information Handling

3.1. Classification of information

An inventory will be maintained of all the PFC's major IT assets and the ownership of each asset will be clearly stated. Within the inventory, the information processed by each IT asset will be classified according to sensitivity.

3.2. Precautions against hardware, software, or data loss

All IT equipment must be safeguarded appropriately, especially when left unattended. Files downloaded from the internet carry a risk and should only be downloaded from trusted sites and scanned with an anti-virus product. Email poses a significant threat and files attached to and links within email must be treated with caution to safeguard against email-based attacks which seek to harvest personal information and deliver malicious code including ransomware that can lead to the encryption of important business data. Spam and Phishing emails received should be reported using email ithelp@pompeyfc.co.uk. IT users have a duty to check the address of the recipient each time an email is sent to reduce the chance of accidental data loss through email.

PFC systems prevent the automatic forwarding of email from PFC accounts. Individuals must avoid sending confidential and sensitive business information from PFC mailboxes to personal email accounts as these accounts are likely to reside in Countries without UK equivalent data protection laws and are therefore inappropriate for certain classifications of PFC data.

The use of USB storage devices is a common cause of compromise through infections from computer viruses, malware and spyware and should be avoided. USB storage devices which are not from a trusted source must not be attached to a PFC computer. Files on trusted USB storage devices must be scanned with an anti-virus product before use or transfer to PFC systems and network drives.

3.3. Disposal of equipment

When permanently disposing of equipment containing all types of storage media, including but not limited to hard disk drives, backup tapes and USB removable media all sensitive or confidential data and licensed software should be irretrievably deleted during the disposal process. Damaged storage devices containing sensitive or confidential data will undergo assessment to determine if the device should be destroyed, repaired or discarded. Such devices will remain the property of PFC and only be removed from site with the permission of the information asset owner. Secure disposal verification certificates should be sought for media which has contained sensitive and confidential data.

3.4. Working practices

PFC advocates a clear screen policy particularly when employees are absent from their workspace and outside normal working hours. Employees must log out or lock their workstations when not in use. Screens on which sensitive or confidential information is processed or viewed should be fitted with a privacy filter or be sited in such a way that they cannot be viewed by unauthorised persons. This applies to both fixed desktops, laptops and mobile devices. Additionally, screens should be positioned so that they are not easily visible through external windows. Whilst sharing screens on video conferencing and collaboration platforms additional care should be taken to ensure sensitive information cannot be viewed by unauthorised persons.

Wherever possible computer applications should be closed before permitting remote access to IT support colleagues undertaking support and maintenance. Individuals must ensure that any screenshots provided to initiate a support ticket or aid with troubleshooting a problem do not contain sensitive and confidential data.

3.5. Off-site removal and cloud storage of data

Removal off-site of PFC's sensitive or confidential information, either in print or held on any type of computer storage medium, including tablets, phones or USB drives whether owned by the PFC or not, should be authorised by your line manager and only in accordance with PFC Data Protection Policy. Cloud storage introduces complexities relating to where data is stored and this is often in Countries without UK equivalent data protection laws. Sensitive or confidential information must not be kept in a cloud storage service which is not approved by PFC. Due diligence must be undertaken to assess the risk to sensitive and confidential data before being uploaded to cloud-based storage and systems.

3.6. Backup and recovery

Backups of PFC's information assets and the ability to recover them are important priorities. Information owners must ensure that system backup and recovery procedures are in place and that these are routinely tested. Backup copies of data must be protected throughout their lifecycle from accidental or malicious alteration and destruction, particularly against the threat of ransomware for which offline, air-gapped, immutable backup technologies provide the strongest safeguards. Access to data backups and supporting infrastructure must be restricted to those persons who are authorised to perform systems administration or management functions. All system managers must ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of datafiles, especially where such files may replace files that are more recent.

3.7. Archiving

The archiving of information must take place with due consideration for legal, regulatory and business issues, with liaison as needed between IT staff, records managers and data owners, and in keeping with PFC's Retention and Disposal Schedule. Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.

3.8. Information lifecycle management

All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files. Day to day data storage must ensure that current information is readily available to authorised users. Any archives created must be accessible in case of need.

3.9. Sensitive or confidential information

Sensitive or confidential data may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured and in accordance with the PFC Data Protection Policy. As a minimum this data must be encrypted in transit and while stored.

Sensitive or confidential data should only be accessed from PFC owned equipment in secure locations and files must never be printed on a networked printer that does not have adequate protection or security. The Using Your Own Device Policy describes the secure use of non-PFC owned equipment.

3.10. Use of electronic communication systems

PFC advocates the use of modern communications methods over email to share information, as described in the Guidance on Managing Emails document. Teams, OneDrive and SharePoint provide greater security through granular access rights management and the ability to revoke access to shared information.

The identity of online recipients, such as email addresses and fax numbers should be checked carefully prior to dispatch, especially where the information content is sensitive or confidential. Verifying the correct document has been attached to an email prior to sending will reduce the opportunity for sensitive data loss via email. In most cases an email and its attachments cannot be revoked once sent externally.

Sensitive or confidential information should only be sent to external recipients via email where modern methods described above are not possible and must be encrypted or protected by a password.

Information received electronically must be treated with care due to its inherent information security risks. Files received from external persons should be scanned for possible viruses or other malicious code.

3.11. Additional data protection declaration requirement

Where a role requires access to specific business systems that contain sensitive personal or financial information, individuals may be required to sign a data protection declaration before they are sanctioned to carry out these duties.

Line managers will make staff aware if they are required to do this and line managers will oversee the process within their department.

4. Mobile and Remote Computing

4.1. Authorisation

Those remotely accessing information systems, data or services containing sensitive or confidential information must be authorised to do so by an appropriate authority, usually the line manager.

4.2. Use of computing equipment off-site

Irrespective of ownership, computers or other devices should only be used off-site for PFC related activities if adequate security controls are in place. Where sensitive or confidential information is being stored or accessed from off-site, an approved access solution, such as UniDesktop, should be used as data then remains within PFC systems.

Where staff owned computers are used sensitive or confidential information must not be stored on the device unless approved by the PFC. The member of staff concerned should take steps to ensure other users of the equipment cannot view or access PFC information. Staff are responsible for ensuring all devices adhere to the highest levels of security as defined in the Bring Your Own Device (BYDO) Policy. As per the BYDO Policy, PFC staff must not use OneDrive client on personally owned devices to access PFC accounts as this systematically synchronises all PFC data to that device, instead, documents residing in OneDrive should be accessed only via a browser.

Any loss or theft of PFC equipment or personal equipment which has been used to access sensitive PFC data must be reported at the earliest opportunity.

Multifactor authentication (MFA) will be enforced on access to PFC systems when being used from off-site. This validates the account holder and reduces the risks relating to weak, shared or compromised passwords.

Public Wi-Fi connections, such as those in hotels and coffee shops, may not be secure and should be avoided. It is trivial for someone to set up a fake Wi-Fi access point with a trusted name to encourage connections which they can then use to view your internet traffic or gain access to your device. Verify the Wi-Fi network with the venue before connecting. If you are unsure of the security of any wired or wireless network, then you should not use it.

4.3. Travelling

Portable computing or storage devices are vulnerable to theft, loss or unauthorised access when travelling and information stored on them should be kept to a minimum. Approved mobile device management software must be installed and activated on PFC owned mobile and portable devices at all times. All devices, including portable storage, must be provided with an appropriate form of access protection including authentication and encryption to prevent unauthorised access to their contents. In addition to passwords, more modern means of authentication such as Touch-ID or Face ID are also acceptable forms of access protection.

Equipment and media should not be left unattended in public places and portable devices should be carried as hand luggage. To reduce the opportunities for unauthorised access, automatic shutdown features should be enabled. Passwords or other similar security tokens for access to the PFC's systems should never be stored on or with the mobile devices they are protecting or in their carrying cases. Screens on which sensitive or confidential information is processed or viewed should be fitted with a privacy filter or be sited in such a way that they cannot be viewed by unauthorised persons.

Export and import controls apply when travelling to certain countries which restrict the use of encrypted devices. Advice should be taken from IT Support before any travel arrangements are made.

5. Outsourcing and Third Party Access

5.1. External suppliers

All external suppliers who have access to PFC IT Systems or data must work under the supervision of PFC staff and in accordance with this Policy. A copy of the Policy will be provided by the system owner to each third-party supplier at the commencement of any new contract or as this policy changes.

Wherever possible supplier remote access accounts should remain disabled by default and enabled temporarily, as required to undertake a specific task, at the request of the system owner or administrator limiting access to agreed timeframes to reduce the opportunity for unauthorised activities that may lead to data loss or unintended disruption. Accounts must be immediately deleted when no longer required.

All activities undertaken by third party suppliers must be agreed in advance.

5.2. Security and confidentiality verification

PFC will assess the risk to its information where accessed, stored or processed by third-party suppliers and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, will require external suppliers of services to satisfy PFC through verification that their security controls, confidentiality practices or contractual clauses reflect our expected standards. This will be the responsibility of the system owner. Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the content and spirit of this Policy.

5.3. Service level agreements

Any facilities management, outsourcing or similar company with which the PFC may do business must be able to demonstrate compliance with the PFC's IT Security Policy and must enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.

6. Operations

6.1. Building access control

Areas and offices where sensitive or confidential information is processed will be given an appropriate level of physical security and access control. Line managers will provide information on the potential security risks and the measures used to control them to staff with authorisation to enter such areas. Line managers must continue to ensure access is appropriate to staff duties and remove access when it is no longer required. Physical access control activity will be logged.

6.2. Operational procedures

System owners must ensure that the procedures for the operation and administration of PFC's business systems and activities are documented and that those procedures and documents are regularly reviewed and maintained. It is particularly important that system owners have robust processes for the approval, creation and usage monitoring of accounts that provide administrative level privileges; as well as regular review and removal of accounts when no longer required.

Duties and areas of responsibility must be segregated to reduce the risk and consequential impact of IT security incidents that might result in financial or other material damage to PFC.

6.3. Procedure for reporting of concerns

System owners must ensure that procedures are established and widely communicated for the reporting to IT Support of security incidents and suspected security weaknesses in PFC's IT Systems. They must also ensure that mechanisms are put in place to monitor and learn from those incidents. Procedures must be established for the reporting of software malfunctions and faults in PFC's IT Systems. Faults and malfunctions must be logged and monitored and timely corrective action taken.

6.4. Change management

Changes to operational procedures, software or hardware must be controlled to ensure continuing compliance with the requirements of this Policy and must have management approval.

Development and testing facilities for business-critical systems will be separated from operational facilities and the migration of software from development to operational status will be subject to formal change control procedures. Development systems should utilise artificial or pseudonymised data and not personal data relating to individuals.

Acceptance criteria for new information systems, upgrades and new versions will be established and suitable tests of the system carried out prior to migration to operational status. Tests

involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place.

6.5. Risk assessment

The security risks to the information assets of all system development projects will be assessed by system owners and access to those assets will be controlled.

6.6. Security Testing

IT systems hosted and maintained by PFC will be periodically tested for known vulnerabilities and weaknesses caused by misconfigured security controls.

Applications hosted and maintained by third party providers, such as cloud Software as a Service (SaaS) systems, must be tested by the vendor at least annually. Proof of testing must be provided by the vendor prior to PFC data being uploaded or entered into the application.

7. User Management

7.1. User identification

System owners must ensure that procedures for the registration and deregistration of users and for managing access to all information systems are established to ensure that all users' access rights match their authorisations. These procedures must be implemented only by suitably trained and authorised staff. All users must have a unique identifier (user ID) for their personal and sole use for access to all of PFC's information services, which should authenticate against the institutional directory where practicable. System owners' procedures must include mechanisms to identify and disable unused user accounts in a timely manner.

7.2. ID security

Actions undertaken on IT systems are recorded and are tied to the user ID used. The user ID must not be used by anyone else and associated passwords must not be shared with any other person for any reason. Password management procedures must be put into place to assist both staff and students in complying with best practice guidelines. Account holders must immediately change their password if they believe it may be known to others or has become compromised. PFC IT will take steps to secure a user account which they believe has been compromised.

7.3. Access control standards

System owners must establish appropriate access control standards for all information systems which minimise information security risks yet allow PFC's business activities to be carried out without undue hindrance. Access to all systems must be authorised by the manager responsible for the system and a record must be maintained of such authorisations, including the appropriate access rights or privileges granted. Procedures must be established for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, staff change their role, or staff or students leave the organisation. Users' access rights must be reviewed at regular intervals.

7.4. Starters, Leavers and Affiliates

Access to PFC IT Systems is only available to employees during their period of employment.

Login credentials must not be shared with new members of staff until their first contracted day.

Line managers must ensure that access to all systems is withdrawn as soon as a staff member's employment is terminated or they transfer to a different role internally. Those requesting Affiliate status must ensure that system access does not extend beyond the requirements of the Affiliate's activities. Those requesting Affiliate status must also ensure that system access is withdrawn as soon as the Affiliate's relationship with PFC ceases. Upon an individual leaving PFC employment or affiliate status PFC equipment and data must be returned and this shall be witnessed and recorded by the line manager.

7.5. User training

All those who wish to access PFC's IT Systems must have successfully completed the training which is deemed appropriate for their role. Advice on what training is required is available from line managers or direct from the team who manages each system (e.g. Ticketmaster, Sage or Microsoft products)

8. System Planning

8.1. Authorisation

New IT Systems, or enhancements to existing systems, must be authorised by IT. The business requirements of all authorised systems must specify appropriate security controls. The implementation of new or upgraded software or hardware must be carefully planned and managed, to ensure that the information security risks associated with such changes are mitigated using a combination of procedural and technical controls.

8.2. Secure Configuration and System Hardening

System owners must ensure that all components of the solution are, and remain configured in a consistently secure manner, including changing all default and publicly known system credentials and application passwords; removal/disablement of all unnecessary accounts, software and services; use of vendor secure configuration guidelines; and undertaking other best practise system hardening techniques.

8.3. Risk assessment and management

System owners must ensure that the information assets associated with any proposed new or updated systems are identified, classified and recorded, and a risk assessment, including, where relevant, a privacy impact assessment, is undertaken to identify the probability and impact of security failure. Equipment supporting business systems must be given adequate protection from unauthorised access, environmental hazards and electrical power failures.

8.4. Access control

System owners must ensure that access controls for all IT Systems are set at appropriate levels in accordance with the value and classification of the information assets being protected. Access to operating system commands and application system functions must be restricted to those persons who are authorised to perform systems administration or management functions. Use of administrative commands and privileges should be logged and monitored wherever practicable.

8.5. Testing

System owners, in consultation with Computing and Library Services, must ensure that prior to acceptance, all new or upgraded systems or hardware are tested to ensure compliance with this Policy, access control standards and requirements for ongoing information security management. For new applications hosted and maintained by third party providers, such as cloud Software as a Service (SaaS) systems proof of security testing must be provided by the vendor prior to PFC data being uploaded or entered into the application.

9. IT Systems Management

9.1. Staffing

IT Systems must be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with individual system owners. All systems management staff must have relevant training in IT security issues.

9.2. Access control

System owners must ensure that access controls are maintained at appropriate levels for all IT Systems and that any changes of access permissions are authorised by the manager of the system or application. A record of access permissions granted must be maintained. Access to all IT Systems must use a secure login process and access may also be limited by time of day or by the location of the initiating terminal, or both.

System owners must ensure that all access to systems containing sensitive or confidential information is logged to identify potential misuse of systems or information. They must also ensure that password management procedures are put into place to ensure the implementation of security procedures and to assist users in complying with best practice guidelines. Default vendor passwords and account credentials must be removed on all new IT equipment and systems prior to deployment.

Remote access to the network must be subject to robust authentication as well as appropriate levels of security. Virtual Private Network (VPN), wireless, and other connections to the network are only permitted for authorised users.

Access to operating system commands must be restricted to those persons who are authorised to perform systems administration or management functions. Use of such commands should be logged and monitored.

9.3. Privileged Access Accounts

System owners and IT staff may have higher privilege or unrestricted access over applications and operating systems to carry out their administrative duties. Accounts with privileged access (including global, domain and local administrator rights) must not be used for day-to-day activities. Non-privileged accounts should be used as default and privileged access rights elevation used only as required. Privileged accounts that provide administrator level access to server and end point operating systems must not be used to read email or access the internet as malware introduced through these common infection routes could then execute with unrestricted access rights. Privilege accounts must provide no more than the rights needed to perform the operation the account is created for, following the principle of least privilege.

Wherever practicable multifactor authentication (MFA) controls must be applied to Administrator and privileged account access to systems.

System owners should routinely review accounts with privileged access and remove access when no longer required.

9.4. Change management

Changes to operational procedures, software or hardware must be controlled to ensure continuing compliance with the requirements of this Policy and have management approval. System owners should employ appropriate mechanisms for the planning, communication and testing of such changes that safeguard the security of systems.

Development and testing facilities for business-critical systems will be separated from operational facilities. Where possible development systems should utilise artificial or pseudonymised data and not personal data relating to individuals, or have security controls which are equivalent to the live system.

Acceptance criteria for new information systems, upgrades and new versions will be established and suitable tests of the system carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place.

All systems developed for or procured within the PFC must follow a formalised development process. The implementation, use or modification of all software on PFC's business systems must be controlled. All software must be checked before implementation to protect against malicious code.

Moves, changes and other reconfigurations of users' network access points will only be carried out by authorised staff.

All changes must be properly tested and authorised before moving to the live environment.

9.5. Network design

PFC data and telecoms network is designed and configured to deliver high performance and reliability to meet PFC's needs whilst providing a high degree of access control and a range of privilege restrictions.

Appropriately configured security devices must be used to protect the networks supporting the PFC's business systems. Firewalls should be used to provide segregation at network boundaries, particularly where the data classification of systems differs. Traffic should be permitted only as required following the principle of least privilege. Firewall policies should be regularly reviewed and removed when no longer required.

Proposed system implementations should include a detailed network design diagram which describes all system components, their role in the solution and the interactions between them. Designs should be validated, and system components installed into the appropriate network for its role.

9.6. Logging

System owners must ensure that where possible security event logs, operational audit logs and error logs are created, properly reviewed and managed by qualified staff. System clocks must be regularly synchronised between PFC's various processing platforms to ensure consistency across log sources.

The logs created by critical servers and security systems will be exported to a Security Information and Event Management (SIEM) system for secure storage, correlation, and to provide real-time analysis.

9.7. System Patching

System owners must ensure that applications they are responsible for remain within vendor support and that these are regularly patched with software security updates to reduce the opportunity for the exploit of known vulnerabilities. Out of support software will never receive security patches for any newly discovered vulnerabilities regardless of severity. Systems owners hold a responsibility for being aware of key system lifecycle dates and to remove or upgrade all software components before vendor support comes to an end.

9.8. Device Management

PFC device management platforms provide broad visibility and control of enrolled IT assets, enhancing the ability to identify system vulnerabilities, providing assessment against compliance baselines, and permitting rapid remediation actions against emerging threats.

PFC owned IT systems must be enrolled into the approved device management platform for that operating system where one exists.

Staff and affiliates may be required to register their personal devices when used for accessing PFC systems in order to collect the minimum information needed to meet the PFC's cyber security certification requirements.