



# Acceptable use of IT Policy

Policy Owner: General Secretary  
Date Approved: 3rd March 2026  
Review Date: March 2029

## 1. Introduction

The UKPSA relies on technology to conduct its business. This Acceptable Use Policy provides guidance to ensure that security is maintained when accessing, processing, or storing UKPSA information, particularly in an environment where most users operate with their own personal devices (Bring Your Own Device - BYOD) and work remotely.

This policy helps all staff, volunteers, third parties, and contractors understand the expected standards for managing UKPSA information and using technologies, including the internet, email, and voice recordings. Adherence is essential to safeguard UKPSA information and maintain its reputation.

## 2. Scope of the Policy

This policy applies to all UKPSA employees, volunteers, agents, contractors, consultants, suppliers, service providers, and business partners throughout the charity who **use, process, store, or transfer UKPSA information**, regardless of whether the device used is owned by the UKPSA or is a personal device.

## 3. Definitions

- **Information:** Any and all data, documents, reports, messages, images, or other materials in hardcopy or electronic format that are created, modified, collected, stored, or transferred for UKPSA business.
- **Technology Resources:** Any computer equipment, electronic devices (laptops, tablets, smartphones), communication systems, and applications used to access or process UKPSA Information. This includes **personal devices** when they are used for UKPSA business.
- **User:** Any individual granted access to UKPSA Information or Technology Resources.



## 4. Risks and Implications

Failure to comply with this policy may expose UKPSA to breaches of confidentiality and information, damage its reputation, and could result in breaches of legislative and regulatory obligations, including those set out by the Charity Commission.

## 5. Reporting a Security Incident

All UKPSA Users must **immediately report** any actual or suspected security incidents to **the association General Secretary**.

Situations to report include, but are not limited to:

1. Loss of Information (electronic or hard copy) or sensitive information sent to the wrong recipient.
2. Alerts from security software (e.g., anti-virus).
3. Breach of information integrity, confidentiality, or availability.
4. Suspicion of a data breach or intent to breach.
5. Loss, theft, or misuse of any device containing UKPSA Information.

## 6. Access Control and Passwords

Access to UKPSA IT and information systems is controlled by unique User IDs and passwords. Individuals are accountable for all actions performed with their credentials. User access is granted with the minimum level necessary to perform a job role (**Principle of Least Privilege**). Elevated access must be approved by the UKPSA General Secretary.

Password Requirements:

- Passwords must not be based on easily guessable personal information (names, birth dates, common dictionary words, user IDs).
- Passwords should include, where possible, a combination of three of the following: alphanumeric upper case, alphanumeric lower case, numeric, and special non-alphanumeric characters.
- Passwords must be hard to guess by others but easy for the owner to remember.
- Passwords for approved third-party platforms **must not** match a user's UKPSA password and should be changed periodically.

Use of User IDs and Passwords:

Individuals **must not**:

- Allow anyone else to use their user ID and password.
- Leave user accounts logged in at an unattended and unlocked computer or device.
- Share or leave their password unprotected (e.g., writing it down).
- Attempt to access data or systems they are not authorised to use or access.



## 7. Internet and Email Conditions of Use

Use of UKPSA internet and email systems is intended for business use. Limited personal use is permitted provided it does not affect business performance, is not detrimental to UKPSA, and does not violate any legal or regulatory obligations.

Individuals **must not**:

- Use webmail or cloud storage locations other than Google Workspace / Bookstack / JustGo for UKPSA business, unless explicitly authorised.
- Use UKPSA systems for harassment, abuse, profanity, obscenities, or derogatory remarks.
- Access, download, send, or receive any data considered offensive, including sexually explicit, discriminatory, defamatory, or libelous material.
- Use the workspace or email for personal financial gain or other private business.
- Send unprotected sensitive or confidential information externally.
- Set up a permanent forward of their UKPSA mail to any personal (non-UKPSA) email account.
- Download copyrighted material without appropriate approval.
- Make adjustments to device security measures or install unauthorised software without approval from the IT Officer (or DPOA/General Secretary as applicable).

## 8. Remote Working, BYOD, and Device Security

The UKPSA operates entirely remotely with no central office, and only a very limited number of individuals are provided with UKPSA laptops. This means that most UKPSA business is conducted using personal devices (Bring Your Own Device - BYOD). The primary responsibility for securing any device (personal or UKPSA-allocated) used to conduct UKPSA business rests with the User. Users working remotely must apply extra vigilance to safeguard UKPSA Information.

### Security Requirements

- **Physical Protection:** Never leave devices unattended in a public place. Secure devices (e.g., lock away, use a cable) and keep them out of sight when not in use or left in a vehicle.
- **Security Software and Configuration:** Immediately report security software alerts to the IT Officer. Do not remove, disable, or alter any anti-virus or security software/settings that would reduce UKPSA Information protection.
- **UKPSA Data Storage:** Use approved platforms only; do not store UKPSA data on unauthorized equipment or cloud services. Mobile devices may require approved Mobile Device Management (MDM) software for security.
- **Remote Access:** Do not provide remote access login credentials to anyone.
- **Hard Copy Security:** Securely manage and store hard copy documents, especially those containing Sensitive/Personally Identifiable Information (PII).

### Reporting

Lost, stolen, or misused devices or documents must be reported **immediately** to the **UKPSA General Secretary**.



## **9. Clear Desk and Clear Screen Policy**

The UKPSA operates a clear desk and clear screen policy to reduce the risk of unauthorised access or loss of information.

- Confidential or restricted Information on paper must be locked away when not required and treated as confidential waste when destroyed .
- Computers and terminals must be left logged off or protected with a screen/keyboard locking mechanism (controlled by a password or equivalent authentication) when unattended.

## **10. Actions upon Termination**

All UKPSA equipment, accounts, and data must be returned to UKPSA at termination. Any UKPSA data or intellectual property developed or gained remains the property of UKPSA and must not be retained or reused for any other purpose beyond termination.

## **11. Monitoring and filtering**

UKPSA has the right to monitor activity on its systems, including internet and email use, in order to ensure its systems security and effective operation, and to protect against misuse. Any monitoring will be carried out in accordance with audited, controlled internal processes, and in accordance with any applicable regulatory requirements.

## **12. Compliance**

UKPSA will regularly assess compliance against this policy. Any violation of this policy may lead to disciplinary measures, up to and including termination of membership.

## **13. Review and Development**

This policy, and any subsidiaries, shall be reviewed by the General Secretary to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations. Additional regulations may be created to cover specific areas.



## Table of Definitions

DPA	Data Protection Act
DPOA	Director of Public Affairs
ICO	Information Commissioners Office
ISP	Information Security Policy
IT	Information Technology
NCSC	National Cyber Security Centre
PII	Personally Identifiable Information
RBAC	Roles Based Access Control
SoA	Statement of Applicability
SyOPs	Security Operating Procedures
UKPSA	United Kingdom Practical Shooting Association

