Forces Online CIO
Unit 5, Workshed Carriage Works
London Street, Swindon
Wiltshire, SN1 5DG.
Telephone: 0300 300 2288
Registered Charity: 1188955 (England & Wales) SC050678 (Scotland)

Forces Online

GDPR Data Protection Policy

Note: This policy is a 'living document' and as such it can be reviewed, revised and amended at any time to meet any changes or amendments deemed necessary to facilitate any legislative or environmental changes, however, such changes will only take place following consultation with and authorisation by the Forces Online CIO, Scotland and Northern Ireland Senior Management team.

GDPR DATA PROTECTION POLICY

Forces Online
www.forcesonline.org.uk

INDEX

---

1. INTRODUCTION AND POLICY STATEMENT

Forces Online is committed to protecting the privacy and personal data of all individuals who engage with our organisation. As a charity supporting the Armed Forces community, we recognise the importance of maintaining trust through responsible data handling.

Our Commitment:

- Full compliance with GDPR and UK Data Protection Act 2018
- Protecting individual privacy rights and freedoms
- Transparent and lawful processing of personal data
- Implementing robust security measures
- Providing accessible mechanisms for exercising data rights
- Continuous improvement of our data protection practices

Policy Objectives:

- Ensure legal compliance with data protection law
- Establish clear procedures for lawful data processing
- Provide guidance for staff on data protection requirements

- Demonstrate accountability and transparency
- Support delivery of charitable objectives whilst protecting privacy

This policy applies to all personal data processed by Forces Online, regardless of format or technology used, covering both automated and manual processing systems.

2. SCOPE AND LEGAL FRAMEWORK

Scope of Application: This policy applies to:

- All staff, volunteers, trustees, contractors, and partners
- All personal data processing activities
- All locations and communication methods
- All data subjects including service users, supporters, staff, and website visitors

Legal Framework:

- General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations
- Human Rights Act 1998
- Relevant charity and sector-specific legislation

Regulatory Authority: The Information Commissioner's Office (ICO) is the UK's data protection authority, responsible for enforcement, guidance, and handling complaints.

3. KEY DEFINITIONS

Personal Data: Any information relating to an identified or identifiable individual, including names, addresses, email addresses, phone numbers, and any other identifying information.

Special Category Data: Sensitive personal data requiring additional protection, including health data, ethnic origin, political opinions, religious beliefs, trade union membership, genetic/biometric data, and data concerning sex life or sexual orientation.

Data Processing: Any operation performed on personal data, including collection, storage, use, disclosure, and deletion.

Data Controller: Forces Online, as we determine the purposes and means of processing personal data.

Data Processor: Third parties who process personal data on our behalf, such as IT service providers.

Data Subject: Any identified or identifiable individual whose personal data we process.

Consent: Freely given, specific, informed, and unambiguous agreement to processing of personal data.

4. DATA PROTECTION PRINCIPLES

All processing must comply with seven key principles:

1. Lawfulness, Fairness and Transparency

- All processing must have a valid lawful basis
- Processing must be fair and not misleading
- Clear information must be provided about processing activities

2. Purpose Limitation

- Data collected for specified, explicit, and legitimate purposes
- No further processing incompatible with original purposes
- New purposes require separate lawful basis

3. Data Minimisation

- Data must be adequate, relevant, and limited to what is necessary
- Regular review to ensure data remains necessary
- No collection of excessive or irrelevant information

4. Accuracy

- Data must be accurate and kept up to date
- Inaccurate data corrected or deleted without delay
- Regular review and verification procedures

5. Storage Limitation

- Data kept only as long as necessary for specified purposes
- Clear retention periods and disposal schedules
- Regular review and deletion of unnecessary data

6. Integrity and Confidentiality

- Appropriate security measures to protect data
- Protection against unauthorised access, loss, or damage
- Regular security assessments and improvements

7. Accountability

- Ability to demonstrate compliance with all principles
- Comprehensive documentation and records
- Regular monitoring and review of practices

5. LAWFUL BASIS FOR PROCESSING

Every processing activity must have a valid lawful basis:

Consent: Freely given, specific, informed agreement

- Used for: Marketing communications, non-essential cookies, optional services
- Requirements: Clear consent requests, easy withdrawal, documented

Contract: Processing necessary for contract performance

- Used for: Service delivery, employment, supplier relationships
- Requirements: Clear contractual necessity, proportionate processing

Legal Obligation: Required by law

- Used for: Charity law compliance, employment law, tax obligations, safeguarding
- Requirements: Clear legal requirement, documented obligation

Vital Interests: Protecting life or preventing serious harm

- Used for: Emergency situations, safeguarding crises
- Requirements: Genuine emergency, no alternative available

Public Task: Carrying out charitable objectives

- Used for: Core charitable activities, public benefit services
- Requirements: Clear charitable purpose, public benefit

Legitimate Interests: Necessary for legitimate business interests

- Used for: Administration, service improvement, fraud prevention
- Requirements: Three-part test (legitimate interest, necessity, balancing test)

6. SPECIAL CATEGORY DATA

Special category data requires additional protection and specific lawful basis:

Types We Process:

- Health information for support services
- Disability data for reasonable adjustments
- Political opinions in advocacy work
- Religious beliefs for chaplaincy services

Additional Lawful Basis Required:

- **Explicit consent:** Higher standard than regular consent
- **Health/social care:** Provision of health or social care services

- **Employment:** Occupational health and employment obligations
- **Substantial public interest:** Charitable activities with appropriate safeguards
- **Vital interests:** Emergency situations where consent cannot be obtained

Enhanced Safeguards:

- Stronger security measures and access controls
- Additional training for staff handling sensitive data
- More restrictive sharing arrangements
- Enhanced breach response procedures
- Regular auditing and monitoring

7. DATA SUBJECT RIGHTS

All individuals have eight key rights under GDPR:

7.1 Right to be Informed

What: Clear information about data processing activities **How:** Privacy notices, direct communication, website information **When:** At point of data collection or within one month if obtained indirectly

7.2 Right of Access

What: Copy of personal data and supplementary information **How:** Written request with identity verification/initial contact through https://welfaresupport.net/contacts/ **Timeframe:** One month from receipt of valid request **Format:** Electronic format (unless otherwise requested)

7.3 Right to Rectification

What: Correction of inaccurate or incomplete personal data **Process:** Assessment of accuracy, correction across all systems, notification to third parties **Timeframe:** One month from request

7.4 Right to Erasure ("Right to be Forgotten")

Grounds: No longer necessary, consent withdrawn, unlawful processing, legal requirement **Exceptions:** Freedom of expression, legal compliance, public interest, legal claims **Process:** Assessment of grounds, secure deletion, third-party notification

7.5 Right to Restrict Processing

Grounds: Accuracy disputed, unlawful processing, no longer needed but required for legal claims, objection pending **Effect:** Data stored but not otherwise processed except with consent or for legal claims

7.6 Right to Data Portability

Scope: Data provided by individual, processed by automated means, based on consent or contract **Format:** Structured, commonly used, machine-readable format **Transmission:** Direct transmission to other controllers where technically feasible

7.7 Right to Object

Direct marketing: Absolute right - must cease immediately **Other processing:** Can continue if compelling legitimate grounds demonstrated **Process:** Assessment of objection, balancing of interests, decision communication

7.8 Automated Decision-Making Rights

Scope: Purely automated decisions with legal or significant effects **Rights:** Human review, explanation of logic, challenge decision **Safeguards:** Meaningful human oversight, bias testing, appeals process

8. PRIVACY NOTICES AND CONSENT

8.1 Privacy Notices

Content Requirements:

- Identity and contact details (including DPO)
- Processing purposes and lawful basis
- Recipients of data and international transfers
- Retention periods and data subject rights
- Complaint procedures and ICO contact details

Format and Accessibility:

- Clear, plain English without technical jargon
- Layered approach with key information prominent
- Multiple formats (website, leaflets, verbal)
- Alternative formats available (large print, audio)

Maintenance:

- Annual comprehensive review
- Updates when processing changes
- Version control and change documentation
- Proactive notification of significant changes

8.2 Consent Management

Obtaining Valid Consent:

- Freely given without coercion
- Specific to particular processing purposes
- Informed with complete information provided
- Unambiguous positive action required

- Separate from other terms and conditions

Children's Consent:

- Under 13: Parental consent required
- 13-17: May give own consent but parents informed
- Age verification and parental responsibility checks
- Child-friendly information and communications

Consent Withdrawal:

- Must be as easy as giving consent
- Available through same channels as original consent
- Immediate effect upon withdrawal
- No negative consequences for withdrawal

9. DATA SECURITY AND ACCESS CONTROLS

9.1 Technical Safeguards

Encryption:

- Data at rest: AES-256 encryption for stored data
- Data in transit: TLS encryption for all transmissions
- Key management: Secure generation, storage, and rotation

Network Security:

- Multi-layered firewall protection
- Intrusion detection and monitoring
- Network segmentation for sensitive data
- Secure VPN for remote access

System Security:

- Regular security updates and patches
- Anti-malware protection on all systems
- Vulnerability scanning and penetration testing
- Secure system configuration and hardening

9.2 Access Controls

Authentication:

- Strong password policies

- Multi-factor authentication for sensitive data access
- Account lockout after failed attempts
- Regular password changes required

Authorisation:

- Role-based access permissions
- Principle of least privilege
- Regular review of access rights
- Formal approval process for access changes

Monitoring:

- Comprehensive access logging
- Real-time monitoring for unusual activity
- Regular audit of access logs
- Automated alerts for suspicious behaviour

9.3 Physical Security

- Secure office premises with access controls
- Locked storage for paper records
- Clean desk policy
- Secure disposal of documents and equipment

10. DATA SHARING AND THIRD PARTIES

10.1 Data Sharing Principles

- Only share data where necessary for legitimate purposes
- Minimum data necessary for specific purpose
- Appropriate lawful basis for sharing
- Clear agreements with all recipients
- Regular monitoring of sharing arrangements

10.2 Third-Party Processors

Selection Criteria:

- Demonstrated data protection expertise
- Appropriate technical and organisational measures
- Good compliance track record

- Relevant certifications (ISO 27001, Cyber Essentials)

Contractual Requirements:

- Clear processing instructions
- Confidentiality obligations
- Security measure specifications
- Sub-processor approval requirements
- Data return/deletion obligations
- Audit rights and breach notification

10.3 International Transfers

Adequacy Decisions: Transfers to countries with adequacy decisions (EU/EEA) **Standard Contractual Clauses:** For transfers to non-adequate countries **Additional Safeguards:** Technical measures where legal protections insufficient **Transfer Impact Assessments:** Risk assessment for transfers to high-risk countries

11. DATA RETENTION AND DISPOSAL

11.1 Retention Principles

- Data kept only as long as necessary
- Clear retention periods for different data types
- Regular review and disposal schedules
- Documentation of retention decisions

11.2 Key Retention Periods

- **Service user records:** 7 years after last contact
- **Staff records:** 6 years after employment ends
- **Financial records:** 7 years after transaction
- **Health records:** 8 years after last treatment
- **Marketing data:** 3 years of no engagement

11.3 Secure Disposal

Electronic Data:

- Secure multi-pass deletion
- Physical destruction of storage media where necessary
- Cryptographic erasure for encrypted data

Paper Records:

- Confidential cross-cut shredding (DIN 66399 P-4 standard)
- Certificates of destruction from approved contractors
- Supervised destruction for highly sensitive documents

12. DATA BREACH MANAGEMENT

12.1 Breach Response Process

Immediate Response (0-4 hours):

- Contain the breach and preserve evidence
- Alert DPO and senior management
- Initial assessment of scope and risks
- Document all actions taken

Investigation (4-24 hours):

- Detailed investigation and root cause analysis
- Full scope determination
- Risk assessment for individuals
- Evidence preservation

Notification (24-72 hours):

- ICO notification if likely risk to individuals (within 72 hours)
- Individual notification if high risk (without undue delay)
- Internal and external communications as appropriate

12.2 Breach Assessment Criteria

High Risk Indicators:

- Special category data involved
- Large numbers of people affected
- Vulnerable individuals (children, elderly)
- Risk of identity theft or fraud
- Potential for discrimination or harm

12.3 Post-Breach Actions

- System recovery and security improvements
- Support for affected individuals
- Comprehensive post-incident review

- Implementation of lessons learned
- Policy and procedure updates

13. TRAINING AND GOVERNANCE

13.1 Training Programme

Mandatory Training:

- GDPR induction for all new staff/volunteers
- Annual refresher training
- Role-specific training for data handling roles
- Specialist training for DPO and investigators

Training Content:

- Legal requirements and principles
- Practical data handling procedures
- Security awareness and incident reporting
- Individual rights and complaint handling

13.2 Governance Structure

Data Protection Officer (DPO):

- Expert knowledge and independence
- Compliance monitoring and advice
- Training delivery and DPIA oversight
- Regulatory liaison and complaint handling

Senior Management:

- Overall accountability for compliance
- Resource provision and culture leadership
- Risk management and performance monitoring
- Board reporting and external accountability

All Staff:

- Personal responsibility for compliance
- Participation in training programmes
- Incident reporting and data security
- Respect for individual rights

13.3 Accountability Measures

- Comprehensive documentation of all processing
- Regular internal audits and compliance checks
- Performance indicators and management reporting
- Independent external reviews
- Continuous improvement programmes

14. MONITORING AND REVIEW

14.1 Performance Monitoring

Key Performance Indicators:

- Training completion rates
- Data subject request response times
- Security incident frequency and severity
- Breach notification compliance
- Audit findings and remediation

14.2 Review Processes

- **Annual Policy Review:** Comprehensive review with stakeholder consultation
- **Quarterly Management Reviews:** Performance assessment and action planning
- **Monthly Reporting:** Brief updates to senior management
- **Incident Reviews:** Immediate review of significant incidents

14.3 Continuous Improvement

- Learning from incidents and complaints
- Adoption of best practices
- Technology updates and process optimisation
- Staff feedback and suggestion schemes
- External benchmarking and peer review

15. CONTACT INFORMATION

Data Protection Officer

- Name: Len Chappell
- Email: len.chappell@forcesonline.org.uk
- Phone: 0300 300 2288

General Data Protection Enquiries

- Email: len.chappell@forcesonline.org.uk
- Phone: 0300 300 2288

Data Subject Rights Requests

- Email: len.chappell@forcesonline.org.uk
- Online: https://forms.office.com/e/emDRV04s6M

Data Protection Complaints

- Email: complaints@forcesonline.org.uk
- Phone: 0300 300 2288

Information Commissioner's Office

- Website: www.ico.org.uk
- Phone: 0303 123 1113

More Information: HERE

APPENDIX A: PRIVACY NOTICE TEMPLATE

Who we are: Forces Online, registered charity supporting the Armed Forces community.

Contact: Unit 5 Workshed Carriage Works, London Street, Wiltshire, SN1 5DG, Tel. 0300 300 2288 len.chappell@forcesonline.org.uk click HERE for further details

Data we collect: Contact details, service history, support needs, health information (where relevant), financial information (where relevant).

How we collect it: Service applications, enquiries, events, website visits, communications.

Why we use it: Provide services, assess eligibility, communicate updates, improve services, legal compliance.

Legal basis: Consent, contract performance, legal obligations, vital interests, public task, legitimate interests.

Who we share with: Other support organisations (with consent), professional advisers, IT providers, regulatory bodies (where required).

How long we keep it: Service records (7 years), financial records (7 years), marketing data (3 years no engagement).

Your rights: Access, rectification, erasure, restriction, portability, objection, automated decision-making rights.

Exercise rights: Contact Unitlen.chappell@forcesonline.org.uk or 0300 300 2288 or online form.

Complaints: Contact DPO or ICO (www.ico.org.uk).

APPENDIX B: DATA SUBJECT REQUEST FORMS

ACCESS REQUEST FORM

- Name, address, contact details
- Proof of identity required
- Specific information requested (if any)
- Time period (if specific)
- Preferred format (email/post)
- Declaration and signature

RECTIFICATION REQUEST FORM

- Personal details
- Current incorrect information
- Correct information
- Supporting evidence
- Declaration and signature

ERASURE REQUEST FORM

- Personal details
- Reason for request (no longer necessary, consent withdrawn, objection, unlawful processing, legal obligation, other)
- Data to be erased (all or specific)
- Declaration and signature

APPENDIX C: DATA RETENTION SCHEDULE

Data Category	Retention Period	Disposal Method
Service User Files	7 years after last contact	Secure Destruction
Staff Records	6 years after leaving	Secure destruction
Financial Records	7 years after last transaction	Secure destruction
Marketing Data	3 years no engagement	Secure destruction
Board Minutes	Permanent archive	N/A
CCTV footage	30 days	Auto-overwrite
System Logs	12 months	Auto-deletion

Review: Annual review of schedule, quarterly disposal activities, monthly monitoring.

Document Control:

- Version: 5.0
- Approved: 07/04/2020
- Review Date: 07/04/2025
- Owner: Data Protection Officer

Forces Online
ICO Registration Number: ZB689910
Charity Registration: 1188955 (England & Wales), SC050678 (Scotland)
www.forcesonline.org.uk

Change Record

Date of Change:	Changed By:	Comments:
07/04/2000	LC/ME	Authorised by Trustees.
07/04/2021	LC/ME	Policy Check
07/04/2022	LC/PE/KS	Policy Check
07/04/2023	LC/PE/KS	Policy Check
07/04/2024	LC/PE/KS	Policy Check
07/04/2025	LC/GD/KS	Policy Check
01/09/2025	LC/KS/SD	Format changed to PDF