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

Confidentiality Policy

CONFIDENTIALITY POLICY

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

INDEX

1. INTRODUCTION AND PURPOSE

Forces Online recognises that confidentiality is fundamental to maintaining trust and providing effective support to the Armed Forces community. As a charity working with military personnel, veterans, and their families, we handle sensitive personal information that requires the highest standards of confidentiality and protection.

This Confidentiality Policy establishes our commitment to protecting confidential information relating to both our beneficiaries and staff members. It provides clear guidance on handling sensitive information whilst enabling us to deliver effective services and maintain professional working relationships.

Why Confidentiality Matters:

- Protects the privacy and dignity of individuals
- Maintains trust and confidence in our services
- Ensures compliance with legal and professional obligations
- Supports effective therapeutic and support relationships
- Protects sensitive military and personal information
- Maintains professional standards and reputation

Key Areas Covered:

- Beneficiary information including health, family, and support needs
- Staff employment, personal, and performance information
- Guidelines for appropriate information sharing
- Security measures for protecting confidential information
- Procedures for handling confidentiality breaches
- Training and awareness requirements

This policy applies to all individuals associated with Forces Online and covers all forms of confidential information, regardless of how it is stored or communicated.

2. POLICY STATEMENT

Forces Online is committed to maintaining the highest standards of confidentiality for all individuals associated with our organisation. We recognise that confidentiality is essential for:

Building and Maintaining Trust: We understand that individuals share sensitive personal information with us in confidence, trusting that we will protect their privacy and use information only for legitimate purposes.

Professional Service Delivery: Confidentiality enables open and honest communication, which is essential for providing effective support, advice, and assistance to the Armed Forces community.

Legal and Ethical Compliance: We are committed to meeting all legal obligations relating to confidentiality and privacy, whilst maintaining the highest ethical standards in our work.

Core Commitments:

Respect for Privacy: We respect the fundamental right to privacy of all individuals and will protect confidential information with appropriate care and attention.

Purpose Limitation: Confidential information will only be used for the specific purposes for which it was provided or for which consent has been given.

Security and Protection: We will implement robust measures to protect confidential information from unauthorised access, disclosure, alteration, or destruction.

Professional Standards: All staff and volunteers will maintain professional standards of confidentiality in accordance with relevant professional codes and best practice.

Transparency and Accountability: We will be transparent about our confidentiality practices and accountable for maintaining appropriate standards of information protection.

Continuous Improvement: We will regularly review and improve our confidentiality practices to ensure they remain effective and appropriate.

This policy reflects our understanding that confidentiality is not absolute and must be balanced with other important considerations, including safeguarding responsibilities, legal obligations, and the need to coordinate effective support services.

3. SCOPE AND APPLICATION

Personnel Covered: This policy applies to all individuals associated with Forces Online, including:

- Permanent and temporary employees
- Volunteers and unpaid helpers
- Trustees, directors, and board members
- Contractors, consultants, and freelancers
- Students and trainees on placement
- Partner organisation representatives
- Third-party service providers with access to confidential information

Information Covered:

- **Beneficiary Information:** All information about service users, including personal circumstances, support needs, health information, family details, and service history
- **Staff Information:** Employment records, personal details, performance information, salary data, and professional development records
- **Organisational Information:** Internal communications, strategic plans, financial information, and operational procedures

- **Third Party Information:** Information received from partner organisations, professional advisers, and other external sources

Circumstances Covered:

- All work-related activities and communications
- Formal and informal discussions about individuals
- Written, electronic, and verbal communications
- Internal meetings and external representation
- Social situations and casual conversations
- Remote working and home-based activities

Geographic Scope: This policy applies regardless of location, including:

- Forces Online premises and facilities
- Home working and remote locations
- Public spaces and transport
- Social events and informal gatherings
- Online and digital communications
- International travel and communications

Duration of Obligations: Confidentiality obligations continue:

- Throughout employment or volunteer relationship
- After leaving Forces Online
- Beyond the end of service relationships with beneficiaries
- Following the death of individuals to whom information relates
- Even when information becomes publicly available through other sources

4. LEGAL FRAMEWORK

Our confidentiality practices are governed by comprehensive legal and regulatory requirements:

Primary Legislation:

- **General Data Protection Regulation (UK GDPR):** Governs processing of personal data and privacy rights
- **Data Protection Act 2018:** UK implementation of GDPR with additional provisions
- **Human Rights Act 1998:** Article 8 right to respect for private and family life
- **Confidentiality of Communications:** Common law duty of confidence

- **Health and Social Care Act 2012:** Specific provisions for health information

Professional Standards:

- Care Quality Commission standards and guidance
- Professional codes of conduct for qualified staff
- NHS Codes of Practice on confidentiality
- Social Care Institute for Excellence guidance
- Charity Commission guidance on information handling

Employment Law:

- Employment Rights Act 1996
- Equality Act 2010
- Public Interest Disclosure Act 1998 (whistleblowing)
- Working Time Regulations 1998
- ACAS Codes of Practice

Safeguarding Legislation:

- Children Act 1989 and 2004
- Care Act 2014
- Mental Capacity Act 2005
- Safeguarding Vulnerable Groups Act 2006
- Counter-Terrorism and Security Act 2015 (Prevent duty)

Other Relevant Law:

- Charity Act 2011
- Proceeds of Crime Act 2002 (anti-money laundering)
- Terrorism Act 2000
- Official Secrets Act 1989 (where applicable)
- Copyright, Designs and Patents Act 1988

Regulatory Guidance:

- Information Commissioner's Office guidance and codes
- Charity Commission guidance on data protection
- Care Quality Commission guidance
- Professional body guidance and standards
- Sector-specific codes of practice

Balancing Conflicting Duties: Where confidentiality duties conflict with other legal obligations (such as safeguarding or crime prevention), we will seek appropriate professional advice and balance competing interests in line with legal requirements and professional guidance.

5. KEY DEFINITIONS

Confidential Information: Any information that is not already in the public domain and which has been provided to Forces Online in circumstances where there is a reasonable expectation that it will be kept confidential.

Personal Information: Any information relating to an identified or identifiable individual, including biographical, circumstantial, and sensitive personal data.

Sensitive Information: Information requiring enhanced protection due to its nature, including health data, financial information, family circumstances, safeguarding concerns, and information about vulnerabilities.

Professional Confidence: Information shared within a professional relationship where there is a legitimate expectation of confidentiality, such as counselling, advice, or support relationships.

Consent: Free, specific, informed, and unambiguous agreement to the sharing or use of confidential information, given by the individual to whom the information relates or their authorised representative.

Need to Know: The principle that confidential information should only be shared with individuals who require access to that information to perform their legitimate duties and responsibilities.

Information Sharing: The disclosure of confidential information to third parties, whether internal or external to the organisation, for specific legitimate purposes.

Data Subject: An individual to whom personal information relates, including current and former beneficiaries, staff members, volunteers, and any other identifiable person.

Authorised Personnel: Individuals who have been specifically authorised to access particular categories of confidential information as part of their role and responsibilities.

Breach of Confidentiality: Any unauthorised access, use, disclosure, alteration, or destruction of confidential information, whether intentional or accidental.

Public Interest: Circumstances where disclosure of confidential information may be justified to prevent harm to individuals or society, subject to careful assessment and appropriate authorisation.

Professional Judgement: The application of professional knowledge, experience, and ethical standards to make decisions about confidentiality in complex or uncertain situations.

Information Security: Technical, physical, and administrative measures designed to protect confidential information from unauthorised access, use, disclosure, alteration, or destruction.

6. PRINCIPLES OF CONFIDENTIALITY

Our approach to confidentiality is based on established principles that guide decision-making and ensure consistent application:

Principle 1: Presumption of Confidentiality All personal information should be treated as confidential unless there are clear reasons to the contrary. This presumption applies regardless of how information is obtained or its apparent sensitivity.

Principle 2: Purpose Limitation Confidential information should only be used for the specific purposes for which it was provided or for which valid consent has been obtained. Using information for other purposes requires separate justification and, where appropriate, additional consent.

Principle 3: Proportionality Any sharing or use of confidential information should be proportionate to the purpose for which it is being shared. Only the minimum amount of information necessary should be disclosed to achieve the legitimate purpose.

Principle 4: Necessity Information sharing should only occur where it is necessary to achieve a legitimate purpose and where that purpose cannot be achieved through less intrusive means.

Principle 5: Accountability All decisions about confidential information should be properly considered, documented, and justifiable. Individuals making such decisions should be prepared to explain and defend their actions.

Principle 6: Transparency Individuals should be informed about how their confidential information will be used and shared, except in circumstances where such disclosure would undermine the purpose of the sharing or create additional risks.

Principle 7: Security Appropriate technical, physical, and administrative measures should be implemented to protect confidential information from unauthorised access, use, disclosure, alteration, or destruction.

Principle 8: Professional Standards All handling of confidential information should meet relevant professional standards and codes of practice applicable to the roles and responsibilities of those involved.

Principle 9: Respect for Individual Rights The rights and interests of individuals to whom confidential information relates should be respected and protected, including their right to privacy, dignity, and autonomy.

Principle 10: Continuous Review Confidentiality arrangements should be regularly reviewed to ensure they remain appropriate, effective, and compliant with changing circumstances and requirements.

7. BENEFICIARY CONFIDENTIALITY

7.1 Service User Information

Types of Information: We collect and maintain various types of information about our beneficiaries to provide effective support services:

Personal Details:

- Full name, date of birth, and contact information
- National Insurance number and identification documents
- Emergency contacts and next of kin information
- Relationship status and household composition

- Nationality, immigration status, and right to services

Service History:

- Military service record and discharge information
- Rank, regiment, and service dates
- Operational deployments and service locations
- Medals, awards, and commendations
- Discharge circumstances and veteran status

Support Needs:

- Reason for referral and presenting issues
- Assessment outcomes and support plans
- Services received and intervention history
- Progress reviews and outcome measures
- Case notes and professional observations

Contact Records:

- Dates and methods of contact
- Details of communications and interactions
- Appointment attendance and cancellations
- Referrals made and received
- Multi-agency meeting participation

Confidentiality Requirements:

- All service user information is confidential by default
- Information should only be accessed by authorised personnel
- Sharing requires valid consent or legal justification
- Security measures must protect against unauthorised access
- Records must be accurate, relevant, and regularly reviewed

Special Considerations for Military Community:

- Military service information may have national security implications
- Operational deployment details require enhanced protection
- Service-related trauma and mental health needs require sensitive handling
- Family separation and deployment stress require careful consideration
- Transition from military to civilian life involves unique confidentiality challenges

7.2 Health and Personal Information

Health Information We May Hold:

- Physical health conditions and medical history
- Mental health diagnoses and treatment history
- Medication information and medical appointments
- Disability information and support needs
- Substance use history and treatment
- Therapy and counselling records

Enhanced Protection Requirements: Health information requires the highest level of confidentiality protection:

- **Access Limitation:** Only personnel directly involved in providing health-related support
- **Secure Storage:** Enhanced security measures for health records
- **Sharing Restrictions:** More stringent consent and justification requirements
- **Professional Standards:** Compliance with healthcare confidentiality codes
- **Retention Periods:** Longer retention periods for health records

Specific Considerations:

- **Mental Health:** Sensitivity around PTSD, depression, and anxiety
- **Service-Related Injuries:** Conditions related to military service may affect compensation claims
- **Substance Use:** Information about alcohol or drug use requires careful handling
- **Domestic Violence:** Health consequences of domestic abuse require safeguarding consideration
- **Sexual Health:** Highly sensitive information requiring enhanced protection

Consent and Sharing:

- Explicit consent generally required for health information sharing
- Emergency situations may justify sharing without consent
- Safeguarding concerns may override normal consent requirements
- Professional healthcare relationships have additional confidentiality obligations
- Insurance and benefits applications may require health information disclosure

7.3 Family and Relationship Information

Family Information We May Hold:

- Spouse/partner details and relationship status
- Children's information including ages, schools, and needs
- Extended family circumstances and support networks
- Relationship difficulties and family conflicts
- Domestic violence history and safety concerns
- Child protection and safeguarding issues

Confidentiality Challenges:

- Information about one family member may affect others
- Children's information requires special protection
- Domestic violence situations require careful risk assessment
- Family conflicts may create competing confidentiality claims
- Multi-generational military families may have complex needs

Sharing Considerations:

- **Family Consent:** May need consent from multiple family members
- **Child Protection:** Overriding duty to protect children from harm
- **Domestic Violence:** Safety considerations may override confidentiality
- **Support Services:** Coordination between different family support services
- **School Information:** Sharing with schools requires careful consideration

Special Protections:

- **Children's Information:** Enhanced protection for under-18s information
- **Domestic Violence:** Specialist confidentiality protocols
- **Family Court:** Information sharing with legal proceedings
- **Social Services:** Mandatory reporting and information sharing requirements
- **Partner Organisations:** Family support service coordination

7.4 Financial Information

Financial Information We May Hold:

- Income, benefits, and financial circumstances
- Debt information and financial difficulties
- Grant applications and financial assistance records
- Pension information and compensation claims
- Banking details for payments and grants

- Housing and accommodation costs

Confidentiality Requirements:

- Financial information is highly sensitive and requires enhanced protection
- Access limited to personnel involved in financial assessment or support
- Sharing requires specific consent or legal justification
- Security measures must prevent financial abuse or fraud
- Regular review to ensure information remains accurate and relevant

Sharing Justifications:

- **Grant Applications:** Sharing with funding bodies and grant providers
- **Debt Advice:** Referral to debt counselling and money advice services
- **Benefits:** Liaison with Department for Work and Pensions
- **Housing:** Sharing with housing providers and local authorities
- **Legal Proceedings:** Court proceedings involving financial matters

Fraud Prevention:

- Verification procedures to prevent fraudulent applications
- Cross-referencing with other sources to ensure accuracy
- Monitoring for unusual patterns or inconsistencies
- Reporting suspected fraud to appropriate authorities
- Cooperation with investigations while maintaining confidentiality

8. STAFF CONFIDENTIALITY

8.1 Employment Information

Types of Employment Information: We maintain comprehensive records about our staff members that require appropriate confidentiality protection:

Personal Details:

- Full name, date of birth, and contact information
- National Insurance number and tax information
- Emergency contacts and next of kin details
- Right to work documentation and visa status
- Bank account details for salary payments

Recruitment Information:

- Application forms and CVs
- Interview notes and assessment records
- Reference checks and employment history
- Criminal record checks and vetting information
- Medical clearance and occupational health records

Employment Terms:

- Contract of employment and job descriptions
- Salary, benefits, and pension information
- Working hours and holiday entitlements
- Probationary period and performance requirements
- Training and development records

Confidentiality Obligations:

- Employment information is confidential to authorised personnel only
- HR team and direct line managers typically have legitimate access
- Sharing requires business justification and appropriate authorisation
- Former employees' information remains confidential after leaving
- Family members and partners have no automatic right to employment information

Access Controls:

- **HR Department:** Full access to employment records for HR purposes
- **Line Managers:** Access to information relevant to management responsibilities
- **Payroll:** Access to financial and payment information only
- **Senior Management:** Access justified by legitimate business needs
- **Trustees:** Access to senior staff information for governance purposes

8.2 Personal Circumstances

Personal Information We May Hold: Staff may share personal information that affects their work or requires support:

Family Circumstances:

- Marital status and family composition
- Children's ages, schools, and care needs
- Elder care responsibilities and family commitments
- Relationship difficulties affecting work performance

- Bereavement and family crisis situations

Health Information:

- Sickness absence records and medical certificates
- Occupational health assessments and recommendations
- Disability information and reasonable adjustments
- Mental health concerns affecting work capacity
- Medical appointments and treatment schedules

Financial Circumstances:

- Financial difficulties affecting work performance
- Salary advance requests and hardship applications
- Court orders affecting salary (e.g., child maintenance)
- Bankruptcy or debt management plans
- Benefits claims and entitlements

Confidentiality Requirements:

- Personal circumstances information requires enhanced protection
- Access limited to those with legitimate need to know
- Sharing requires explicit consent except in exceptional circumstances
- Support and assistance should be provided sensitively and confidentially
- Records should be kept separate from general employment files where appropriate

Support Provision:

- **Employee Assistance Programmes:** Confidential counselling and support services
- **Flexible Working:** Arrangements to accommodate personal circumstances
- **Special Leave:** Compassionate leave and time off for personal matters
- **Occupational Health:** Confidential assessment and support services
- **Financial Support:** Hardship funds and salary advances where appropriate

8.3 Performance and Disciplinary Matters

Performance Information:

- Annual performance reviews and appraisals
- Personal development plans and objectives
- Training needs analysis and development records
- Supervision notes and feedback sessions

- Achievement recognition and awards

Disciplinary Information:

- Disciplinary investigation records
- Grievance procedures and outcomes
- Misconduct allegations and responses
- Formal warnings and disciplinary sanctions
- Appeal procedures and decisions

Confidentiality Requirements:

- Performance and disciplinary information is highly confidential
- Access strictly limited to those directly involved in the process
- Information should not be discussed with colleagues or external parties
- Records must be securely stored with appropriate access controls
- Information should be factual, fair, and properly documented

Sharing Limitations:

- **Need to Know:** Only those directly involved in management or HR processes
- **Legal Requirements:** Disclosure may be required for legal proceedings
- **Regulatory Inquiries:** Information may need to be shared with regulators
- **Reference Requests:** Limited factual information may be provided in references
- **Appeals:** Information may need to be shared with appeal panel members

Protection Measures:

- Separate storage for disciplinary records
- Time-limited access to investigation materials
- Anonymisation where possible in policy development
- Clear retention and disposal schedules
- Training for managers on confidentiality requirements

8.4 Salary and Benefits Information

Financial Information We Hold:

- Basic salary and any additional payments
- Overtime, expenses, and allowance information
- Pension contributions and entitlements
- Benefits in kind and their values

- Tax codes and PAYE information
- Salary sacrifices arrangements

Confidentiality Requirements:

- Salary information is highly confidential and sensitive
- Access limited to payroll, HR, and authorised managers
- Sharing requires explicit authorisation from senior management
- Comparisons between staff salaries should be avoided
- Information should not be disclosed to colleagues or external parties

Legitimate Sharing:

- **HMRC:** Tax and National Insurance reporting requirements
- **Pension Providers:** Contributions and member information
- **Auditors:** Financial audit and compliance requirements
- **Legal Proceedings:** Court orders and employment tribunal cases
- **Benefits Agencies:** Information for benefit and tax credit assessments

Protection Measures:

- Secure payroll systems with restricted access
- Confidential handling of salary-related communications
- Separate storage of salary and benefits information
- Regular review of access permissions
- Clear procedures for handling salary queries and disputes

9. INFORMATION SHARING GUIDELINES

9.1 When Information May Be Shared

Information sharing is essential for effective service delivery and coordination, but must be conducted within appropriate frameworks:

Legitimate Purposes for Sharing:

- **Service Coordination:** Sharing between team members providing support to the same individual
- **Referral Processes:** Providing information to other services or organisations to facilitate appropriate referrals
- **Multi-Agency Working:** Coordinating support with other agencies working with the same family or individual
- **Professional Supervision:** Sharing information for case supervision, professional guidance, and quality assurance

- **Quality Assurance:** Anonymised or pseudonymised information for service evaluation and improvement
- **Safeguarding:** Sharing information to protect individuals from harm or abuse
- **Legal Requirements:** Disclosure required by law, court order, or regulatory requirement

Assessment Framework: Before sharing information, staff must consider:

1. **Is sharing necessary?** Can the purpose be achieved without sharing confidential information?
2. **What is the purpose?** Clear identification of why information needs to be shared
3. **Is consent available?** Has the individual consented to sharing, or is consent required?
4. **Is sharing proportionate?** Is the amount of information being shared proportionate to the purpose?
5. **Is sharing lawful?** Does sharing comply with data protection and confidentiality requirements?
6. **Are recipients appropriate?** Are the recipients legitimate and appropriate for receiving the information?
7. **Is sharing secure?** Will the information be transmitted and stored securely?

9.2 Consent and Authorisation

Valid Consent Requirements:

- **Free:** Given without coercion, pressure, or negative consequences for refusal
- **Informed:** Individual understands what information will be shared, with whom, and for what purpose
- **Specific:** Consent relates to specific information and specific sharing arrangements
- **Current:** Consent is current and has not been withdrawn
- **Capable:** Individual has capacity to give consent or appropriate person consents on their behalf

Obtaining Consent:

- **Explanation:** Clear explanation of what information will be shared and why
- **Documentation:** Written record of consent obtained and any limitations specified
- **Ongoing:** Regular review to ensure consent remains current and appropriate
- **Withdrawal:** Clear process for withdrawing consent and implications explained
- **Capacity:** Assessment of individual's capacity to give informed consent

When Consent is Not Required:

- **Legal Obligation:** Sharing required by law (e.g., safeguarding, court orders)
- **Vital Interests:** Sharing necessary to protect life or prevent serious harm
- **Public Interest:** Sharing justified by substantial public interest
- **Legitimate Interests:** Sharing necessary for legitimate organisational or professional purposes

Special Consent Considerations:

- **Children:** Parental consent may be required for under-16s, depending on capacity
- **Mental Capacity:** Capacity assessment required for individuals with mental health or learning difficulties
- **Family Information:** Consent may be needed from multiple family members
- **Third Party Information:** Consent from all individuals to whom shared information relates
- **Professional Relationships:** Enhanced consent requirements for therapeutic relationships

Consent Documentation:

- Date, time, and method of consent
- Specific information to be shared
- Recipients of information
- Purpose of sharing
- Any limitations or conditions
- Duration of consent
- Right to withdraw consent

9.3 Safeguarding Disclosures

Safeguarding Obligations: We have legal and moral obligations to protect individuals from harm, which may override normal confidentiality requirements:

Child Protection:

- Duty to report suspected child abuse or neglect
- Sharing information with social services and police
- Multi-agency safeguarding procedures
- Court proceedings and child protection conferences
- Information sharing with schools and health services

Adult Safeguarding:

- Protecting vulnerable adults from abuse, neglect, or exploitation
- Sharing with adult social care and safeguarding boards
- Mental capacity assessments and best interests decisions
- Domestic violence protection and safety planning
- Financial abuse prevention and reporting

Risk Assessment:

- **Immediacy:** Immediate risk requires immediate information sharing
- **Severity:** Serious harm justifies overriding confidentiality
- **Likelihood:** Probable harm requires preventive action
- **Vulnerability:** Additional protection for vulnerable individuals
- **Professional Judgement:** Experienced assessment of risk factors

Safeguarding Information Sharing:

- Share information proportionate to the risk
- Document decisions and rationale for sharing
- Inform individuals about sharing where possible and safe
- Coordinate with other agencies appropriately
- Follow up to ensure appropriate action taken

Documentation:

- Detailed records of concerns and evidence
- Decision-making process and rationale
- Information shared and with whom
- Follow-up actions and outcomes
- Professional consultations and advice received

9.4 Legal Requirements

Mandatory Disclosure: Certain circumstances require disclosure of confidential information regardless of consent:

Court Orders:

- Subpoenas and witness summons
- Disclosure orders in legal proceedings
- Family court proceedings involving children

- Criminal proceedings and police investigations
- Employment tribunal cases

Regulatory Requirements:

- Charity Commission inquiries
- Care Quality Commission inspections
- Information Commissioner's Office investigations
- Health and Safety Executive investigations
- Financial services regulatory requirements

Statutory Obligations:

- **Terrorism Prevention:** Prevent duty reporting requirements
- **Money Laundering:** Suspicious activity reporting
- **Safeguarding:** Child and adult protection reporting
- **Health and Safety:** Incident reporting requirements
- **Employment Law:** Discrimination and harassment investigations

Professional Standards:

- Professional body investigations
- Fitness to practice proceedings
- Registration and licensing requirements
- Quality assurance and audit processes
- Complaints and disciplinary procedures

Response Procedures:

1. **Verify Legitimacy:** Confirm the legal basis and authority for the request
2. **Seek Advice:** Obtain legal or professional advice if uncertain
3. **Limit Disclosure:** Provide only information specifically required
4. **Document Process:** Maintain records of disclosure and rationale
5. **Inform Individuals:** Notify affected individuals where possible and appropriate
6. **Follow Up:** Monitor use of disclosed information where possible

10. HANDLING CONFIDENTIAL INFORMATION

10.1 Storage and Security

Physical Security:

- **Locked Storage:** All confidential paper records stored in locked filing cabinets or secure storage areas
- **Access Controls:** Keys and access codes limited to authorised personnel only
- **Clean Desk Policy:** Confidential documents not left on desks or in open areas
- **Visitor Controls:** Confidential information secured when visitors are present
- **Transport Security:** Secure procedures for transporting confidential documents

Document Management:

- **File Organisation:** Clear filing systems with appropriate categorisation
- **Version Control:** Current versions clearly identified and obsolete versions securely destroyed
- **Retention Schedules:** Regular review and disposal in accordance with retention policies
- **Archive Management:** Long-term storage with appropriate access controls and environmental protection
- **Destruction Procedures:** Secure destruction using cross-cut shredding or approved destruction services

Environmental Security:

- **Office Security:** Premises secured outside working hours with appropriate alarm systems
- **Working Areas:** Confidential work conducted in appropriate areas away from public access
- **Meeting Rooms:** Confidential meetings conducted in private rooms with appropriate sound insulation
- **Telephone Conversations:** Private areas for confidential telephone conversations
- **Public Spaces:** Confidential information not discussed or accessed in public areas

10.2 Access Controls

Need to Know Principle: Access to confidential information is restricted to individuals who need the information to perform their legitimate duties and responsibilities.

Authorisation Levels:

- **Direct Service Provider:** Access to information about individuals they are directly supporting
- **Line Manager:** Access to team information and supervision-related records
- **HR Personnel:** Access to employment-related information for HR purposes
- **Senior Management:** Access justified by management responsibilities and oversight duties

- **Trustees:** Access to governance-related information and serious incident reports

Access Management:

- **User Accounts:** Individual user accounts with appropriate permission levels
- **Regular Review:** Quarterly review of access permissions and user accounts
- **Role Changes:** Immediate adjustment of access when roles change
- **Leavers:** Prompt removal of access when individuals leave the organisation
- **Audit Trails:** Comprehensive logging of access to confidential information

Special Categories:

- **Health Records:** Access limited to qualified health professionals and direct care staff
- **Safeguarding Files:** Enhanced access controls with senior management oversight
- **Disciplinary Records:** Access limited to HR and management personnel directly involved
- **Financial Information:** Access restricted to finance team and authorised managers
- **Legal Files:** Access limited to legal team and senior management as appropriate

10.3 Communication and Discussion

Professional Discussions:

- **Appropriate Settings:** Confidential matters discussed in private settings away from others
- **Relevant Participants:** Only individuals with legitimate need to know included in discussions
- **Purpose Focus:** Discussions focused on legitimate professional purposes
- **Documentation:** Important discussions documented appropriately with consent where required
- **Follow-Up:** Clear agreements about any actions or further communications

Supervision and Consultation:

- **Professional Supervision:** Regular supervision sessions for case discussion and professional development
- **Peer Consultation:** Appropriate consultation with colleagues for professional advice and support
- **External Consultation:** Consultation with external professionals with appropriate consent and confidentiality agreements
- **Anonymous Discussion:** Use of anonymous or pseudonymised cases for training and development
- **Record Keeping:** Appropriate records of supervision and consultation discussions

Informal Communications:

- **Corridor Conversations:** Confidential matters not discussed in corridors or public areas
- **Social Settings:** No discussion of confidential information in social or informal settings
- **Family and Friends:** Confidential information not discussed with family members or personal friends
- **Public Transport:** No discussion of confidential information on public transport or in public spaces
- **Break Areas:** Confidential information not discussed in staff break rooms or communal areas

Communication Standards:

- **Professional Language:** Appropriate and respectful language used in all communications
- **Factual Accuracy:** Information communicated should be accurate and verified
- **Objective Reporting:** Personal opinions separated from factual information
- **Cultural Sensitivity:** Communications show respect for cultural and religious diversity
- **Non-Discriminatory:** Communications free from discrimination, bias, or prejudice

10.4 Record Keeping

Documentation Standards:

- **Accuracy:** All records must be factually accurate and based on verified information
- **Relevance:** Records should contain only information relevant to the purpose for which they are maintained
- **Timeliness:** Records updated promptly after events or interactions
- **Objectivity:** Records should be objective and professional, avoiding personal opinions or judgements
- **Completeness:** Records should contain sufficient information to support decision-making and continuity of care

Record Creation:

- **Authorised Personnel:** Only authorised staff create records in individual files
- **Professional Standards:** Records meet professional standards and codes of practice
- **Clear Attribution:** All entries clearly attributed to the person making the record
- **Date and Time:** All entries dated and timed appropriately
- **Corrections:** Errors corrected appropriately without obscuring original entries

Record Maintenance:

- **Regular Review:** Files reviewed regularly to ensure accuracy and relevance
- **Update Procedures:** Clear procedures for updating information and adding new records
- **Version Control:** Clear identification of current versions and superseded information
- **Quality Assurance:** Regular quality checks on record keeping standards
- **Training:** Ongoing training for staff on record keeping requirements

Record Retention:

- **Retention Schedules:** Clear schedules for how long different types of records are retained
- **Review Periods:** Regular review to determine whether records are still needed
- **Disposal Procedures:** Secure disposal of records no longer required
- **Archive Management:** Appropriate long-term storage for records with historical value
- **Legal Requirements:** Compliance with legal requirements for record retention

11. DIGITAL AND ELECTRONIC CONFIDENTIALITY

11.1 Email and Electronic Communications

Email Security:

- **Encryption:** Confidential information sent by encrypted email where possible
- **Secure Systems:** Use of approved organisational email systems for confidential communications
- **Recipient Verification:** Careful verification of recipient email addresses before sending
- **Subject Lines:** Generic subject lines that do not reveal confidential information
- **Attachment Security:** Password protection or encryption for confidential attachments

Electronic Communication Guidelines:

- **Professional Accounts:** Use of professional email accounts rather than personal accounts for work communications
- **Auto-Forward:** No automatic forwarding of emails containing confidential information to external accounts
- **Distribution Lists:** Careful use of distribution lists to avoid inappropriate sharing

- **Reply All:** Caution with "reply all" to avoid unintended disclosure
- **Email Retention:** Appropriate retention and deletion of emails containing confidential information

Mobile and Remote Communications:

- **Secure Connections:** Use of secure networks and VPN connections for remote access
- **Device Security:** Password protection and encryption on mobile devices
- **Public Wi-Fi:** No access to confidential information over unsecured public wireless networks
- **Location Awareness:** Awareness of surroundings when accessing confidential information remotely
- **Lost Devices:** Immediate reporting and remote wiping procedures for lost or stolen devices

11.2 Digital Records and Databases

Database Security:

- **Access Controls:** Role-based access controls with individual user accounts
- **Password Security:** Strong passwords and regular password changes
- **Multi-Factor Authentication:** Additional security layers for sensitive systems
- **Session Management:** Automatic logout after periods of inactivity
- **Audit Trails:** Comprehensive logging of all database access and changes

Data Entry and Management:

- **Accuracy:** Careful data entry with verification procedures
- **Completeness:** Ensuring all required fields are completed accurately
- **Consistency:** Consistent data entry standards and formats
- **Updates:** Timely updates when information changes
- **Quality Control:** Regular checks on data quality and accuracy

System Maintenance:

- **Regular Backups:** Frequent secure backups of confidential databases
- **Software Updates:** Regular application of security updates and patches
- **Vulnerability Management:** Regular security scanning and vulnerability assessments
- **Access Review:** Regular review of user access rights and permissions
- **System Monitoring:** Continuous monitoring for unusual activity or security breaches

11.3 Remote Working and Mobile Devices

Home Working Security:

- **Secure Environment:** Private workspace at home for confidential work
- **Family Access:** Preventing access by family members to confidential information
- **Visitor Security:** Securing confidential information when visitors are present
- **Equipment Security:** Appropriate storage and security for work equipment
- **Network Security:** Secure home internet connections and router configurations

Mobile Device Management:

- **Device Registration:** All devices accessing confidential information registered with IT department
- **Security Software:** Appropriate security software installed and regularly updated
- **Remote Wipe:** Capability to remotely wipe devices if lost or stolen
- **Personal Use:** Clear separation between work and personal use of devices
- **Disposal:** Secure data wiping before disposal or recycling of devices

Cloud Services and Online Platforms:

- **Approved Services:** Use of approved cloud services and online platforms only
- **Data Location:** Understanding of where data is stored geographically
- **Access Controls:** Appropriate access controls and permission settings
- **Sharing Settings:** Careful configuration of sharing and collaboration settings
- **Service Monitoring:** Regular review of cloud service security and compliance

12. THIRD PARTIES AND EXTERNAL PARTNERS

12.1 Information Sharing Agreements

Formal Agreements: All information sharing with external parties must be governed by appropriate formal agreements:

Data Sharing Agreements: Comprehensive agreements covering:

- Purpose and scope of information sharing
- Types of information to be shared
- Legal basis for sharing
- Security and confidentiality requirements
- Access controls and authorised personnel
- Retention and disposal arrangements
- Review and termination procedures

Service Level Agreements: For service providers accessing confidential information:

- Specific confidentiality clauses and obligations
- Security standards and requirements
- Staff training and awareness requirements
- Incident reporting and breach notification
- Audit rights and compliance monitoring
- Liability and indemnification provisions

Memoranda of Understanding: For partnership working arrangements:

- Clear roles and responsibilities
- Information sharing protocols
- Confidentiality and security standards
- Dispute resolution procedures
- Review and amendment processes

12.2 Professional Services

Legal Advisers:

- Professional privilege protections
- Clear instructions on confidentiality requirements
- Appropriate non-disclosure agreements
- Secure communication channels
- Document handling and storage requirements

Accountants and Auditors:

- Professional confidentiality obligations
- Access limited to necessary financial information
- Secure handling of financial records
- Clear reporting and communication procedures
- Appropriate data retention and disposal

Consultants and Contractors:

- Comprehensive confidentiality agreements
- Security clearance requirements where appropriate
- Limited access to necessary information only
- Supervision and monitoring arrangements

- Clear termination and information return procedures

IT Service Providers:

- Enhanced security requirements for system access
- Clear data processing agreements
- Technical and organisational security measures
- Regular security assessments and audits
- Incident response and breach notification procedures

12.3 Referrals and Partnerships

Referral Procedures:

- **Consent:** Appropriate consent for information sharing with referral agencies
- **Necessary Information:** Sharing only information necessary for referral purpose
- **Secure Transmission:** Using secure methods for transmitting referral information
- **Follow-Up:** Monitoring outcomes and maintaining ongoing communication
- **Feedback:** Receiving appropriate feedback on referral outcomes

Multi-Agency Working:

- **Information Sharing Protocols:** Clear agreements on information sharing in multi-agency cases
- **Lead Agency:** Clear identification of lead agency and coordination responsibilities
- **Regular Review:** Regular review meetings with appropriate information sharing
- **Conflict Resolution:** Procedures for resolving conflicts over information sharing
- **Quality Assurance:** Monitoring quality and effectiveness of multi-agency working

Partnership Arrangements:

- **Strategic Partnerships:** Formal agreements governing information sharing in strategic partnerships
- **Operational Partnerships:** Day-to-day arrangements for sharing information in operational partnerships
- **Joint Services:** Shared confidentiality standards for jointly delivered services
- **Co-location:** Arrangements for maintaining confidentiality in co-located services
- **Shared Systems:** Security and confidentiality arrangements for shared IT systems

13. BREACHES OF CONFIDENTIALITY

13.1 Types of Breaches

Intentional Breaches:

- Deliberate unauthorised disclosure of confidential information
- Malicious sharing of information for personal gain
- Inappropriate curiosity leading to unauthorised access
- Revenge or retaliation through information disclosure
- Commercial exploitation of confidential information

Accidental Breaches:

- Misdirected emails or letters containing confidential information
- Documents left in inappropriate locations
- Conversations overheard in public areas
- Information displayed on screens visible to others
- Incorrect disposal of confidential documents

System Breaches:

- Unauthorised access to computer systems
- Hacking or cyber-attacks on confidential databases
- Malware or virus infections compromising confidential information
- System failures leading to inappropriate information exposure
- Cloud service breaches affecting confidential data

Process Breaches:

- Failure to follow proper information sharing procedures
- Inadequate consent procedures for information sharing
- Inappropriate retention of confidential information
- Failure to implement appropriate access controls
- Inadequate training leading to confidentiality failures

13.2 Reporting Procedures

Immediate Reporting: All suspected or confirmed breaches of confidentiality must be reported immediately:

Internal Reporting:

1. **Line Manager:** Report to immediate line manager within 2 hours of discovery
2. **Data Protection Officer:** Notify DPO immediately for all personal data breaches
3. **Senior Management:** Alert senior management for serious breaches
4. **Incident Log:** Record breach in organisational incident log

5. **Investigation Team:** Assemble appropriate investigation team

External Reporting: Where required by law or professional standards:

- **ICO Notification:** Personal data breaches within 72 hours if high risk
- **Professional Bodies:** Notification to relevant professional regulatory bodies
- **Police:** Criminal breaches reported to appropriate law enforcement
- **Charity Commission:** Serious incidents reported as required
- **Insurance:** Notification to professional indemnity insurers

Documentation Requirements:

- Date, time, and circumstances of discovery
- Nature and extent of the breach
- Information involved and individuals affected
- Cause of the breach and contributing factors
- Immediate actions taken to contain the breach
- Assessment of potential harm to individuals
- Actions planned to prevent recurrence

13.3 Investigation and Response

Investigation Process:

1. **Containment:** Immediate action to prevent further unauthorised disclosure
2. **Assessment:** Evaluation of scope and severity of breach
3. **Evidence Gathering:** Collection and preservation of relevant evidence
4. **Interviews:** Interviews with relevant staff and witnesses
5. **Root Cause Analysis:** Investigation of underlying causes and contributing factors
6. **Impact Assessment:** Assessment of harm caused to affected individuals
7. **Remedial Action:** Implementation of measures to address breach consequences

Individual Notification: Affected individuals must be notified where:

- There is significant risk of harm from the breach
- Legal or regulatory requirements mandate notification
- Professional standards require individual notification
- Transparency and trust considerations support notification

Support for Affected Individuals:

- Clear explanation of what happened and what information was involved

- Practical advice on steps individuals can take to protect themselves
- Ongoing support and monitoring for potential consequences
- Access to counselling or other support services where appropriate
- Compensation or redress where harm has been caused

Disciplinary Action: Where breaches result from individual misconduct:

- Investigation in accordance with disciplinary procedures
- Appropriate disciplinary sanctions depending on severity
- Additional training and support where appropriate
- Performance monitoring and support plans
- Professional body notification where required

13.4 Prevention and Mitigation

Risk Assessment:

- Regular assessment of confidentiality risks across all operations
- Identification of high-risk activities and processes
- Assessment of technical, physical, and administrative vulnerabilities
- Regular review and updating of risk assessments
- Integration of confidentiality risks into overall risk management

Preventive Measures:

- **Technical Controls:** Robust IT security and access controls
- **Physical Security:** Appropriate physical security measures
- **Training:** Comprehensive confidentiality training for all staff
- **Policies:** Clear policies and procedures covering all aspects of confidentiality
- **Monitoring:** Regular monitoring and audit of confidentiality practices

Continuous Improvement:

- Learning from breaches and near-miss incidents
- Regular review and update of confidentiality procedures
- Benchmarking against best practice in other organisations
- Staff feedback and suggestions for improvement
- External review and assessment of confidentiality practices

14. TRAINING AND AWARENESS

Mandatory Training Programme:

Induction Training: All new staff, volunteers, and trustees receive comprehensive confidentiality training within their first month, covering:

- Legal and professional obligations relating to confidentiality
- Organisational policies and procedures
- Practical guidance on handling confidential information
- Information sharing guidelines and consent procedures
- Recognition and reporting of confidentiality breaches
- Specific requirements for their role and responsibilities

Annual Refresher Training: All personnel receive annual refresher training including:

- Updates to legal requirements and professional standards
- Changes to organisational policies and procedures
- Lessons learned from confidentiality incidents
- Emerging risks and new technologies
- Case studies and practical exercises
- Assessment of knowledge and understanding

Role-Specific Training:

Service Delivery Staff:

- Enhanced training on beneficiary confidentiality
- Professional relationship boundaries and confidentiality
- Information sharing in multi-agency working
- Consent procedures and capacity assessment
- Safeguarding and confidentiality balance
- Record keeping and documentation standards

Management Staff:

- Staff confidentiality and employment law
- Disciplinary and performance management confidentiality
- Information sharing with senior management and trustees
- Breach investigation and response procedures
- Confidentiality in recruitment and selection
- Managing confidentiality in supervision and appraisal

Administrative Staff:

- Handling confidential documents and records
- Telephone and reception confidentiality
- Email and electronic communication security
- Filing and record management systems
- Visitor management and information security
- Database and system access controls

IT and Technical Staff:

- Technical security measures for confidential information
- Database and system administration confidentiality
- Backup and disaster recovery procedures
- Incident response and forensic procedures
- Cloud services and third-party confidentiality
- System monitoring and audit trail management

Training Methods:

- Interactive workshops and seminars
- Online learning modules and assessments
- Case study discussions and role-playing exercises
- Professional supervision and mentoring
- External training courses and conferences
- Peer learning and knowledge sharing sessions

Training Evaluation:

- Pre and post-training knowledge assessments
- Practical competency assessments
- Regular feedback from participants
- Monitoring of confidentiality incident rates
- Annual review of training effectiveness
- Continuous improvement based on evaluation results

15. RESPONSIBILITIES

15.1 Organisational Responsibilities

Forces Online has overall responsibility for:

- **Policy Development:** Developing and maintaining comprehensive confidentiality policies
- **Resource Provision:** Providing adequate resources for confidentiality training and systems
- **Culture Leadership:** Promoting a culture of respect for confidentiality
- **Compliance Monitoring:** Monitoring compliance with confidentiality requirements
- **System Security:** Implementing and maintaining appropriate security systems
- **Legal Compliance:** Ensuring compliance with all legal and regulatory requirements
- **Incident Response:** Establishing effective procedures for responding to confidentiality breaches
- **Continuous Improvement:** Regular review and improvement of confidentiality practices

15.2 Management Responsibilities

Managers at all levels are responsible for:

- **Team Leadership:** Leading by example in maintaining confidentiality standards
- **Staff Supervision:** Supervising staff compliance with confidentiality requirements
- **Training Provision:** Ensuring staff receive appropriate confidentiality training
- **Incident Management:** Managing confidentiality incidents within their areas
- **Policy Implementation:** Implementing confidentiality policies and procedures effectively
- **Performance Management:** Managing performance issues relating to confidentiality
- **Resource Management:** Ensuring adequate resources for maintaining confidentiality
- **Communication:** Communicating confidentiality requirements clearly to staff

Line Manager Specific Duties:

- Conducting confidentiality briefings for new team members
- Regular supervision discussions about confidentiality matters
- Monitoring team compliance with confidentiality procedures
- Providing guidance and support on confidentiality issues
- Reporting confidentiality concerns and incidents promptly
- Participating in confidentiality breach investigations
- Implementing corrective actions following incidents

15.3 Staff Responsibilities

All staff members, volunteers, and associated personnel are responsible for:

- **Personal Compliance:** Maintaining confidentiality in all their activities
- **Professional Standards:** Meeting professional standards and codes of practice
- **Training Participation:** Participating fully in confidentiality training programmes
- **Incident Reporting:** Reporting confidentiality concerns and breaches promptly
- **Information Security:** Maintaining appropriate security for confidential information
- **Consent Procedures:** Following proper consent procedures for information sharing
- **Record Keeping:** Maintaining accurate and secure records
- **Continuous Learning:** Keeping up to date with confidentiality requirements and best practice

Individual Professional Duties:

- Understanding confidentiality requirements for their specific role
- Seeking guidance when uncertain about confidentiality requirements
- Challenging poor confidentiality practice by colleagues
- Supporting colleagues in maintaining confidentiality standards
- Reflecting on their own confidentiality practice and seeking improvement
- Maintaining confidentiality even after leaving the organisation

15.4 Trustee Responsibilities

The Board of Trustees is responsible for:

- **Governance Oversight:** Providing governance oversight of confidentiality arrangements
- **Policy Approval:** Approving confidentiality policies and significant changes
- **Risk Management:** Overseeing confidentiality risks as part of overall risk management
- **Performance Review:** Reviewing organisational performance on confidentiality matters
- **Resource Allocation:** Ensuring adequate resources for confidentiality requirements
- **Legal Compliance:** Ensuring organisational compliance with legal and regulatory requirements
- **Incident Oversight:** Overseeing response to serious confidentiality incidents
- **External Accountability:** Representing the organisation's confidentiality commitments externally

Individual Trustee Duties:

- Understanding their own confidentiality obligations as trustees
- Maintaining confidentiality of sensitive board discussions and decisions
- Challenging management on confidentiality performance where necessary
- Supporting management in improving confidentiality arrangements
- Participating in relevant training and development on confidentiality issues
- Acting as ambassadors for the organisation's confidentiality commitments

16. MONITORING AND COMPLIANCE

Performance Monitoring: We monitor confidentiality performance through:

- **Incident Tracking:** Recording and analysing all confidentiality incidents
- **Training Metrics:** Monitoring training completion rates and assessment results
- **Audit Activities:** Regular internal and external audits of confidentiality practices
- **Compliance Checks:** Regular verification of compliance with policies and procedures
- **Staff Feedback:** Collecting feedback from staff on confidentiality arrangements
- **User Feedback:** Monitoring feedback from service users and other stakeholders

Key Performance Indicators:

- Number and severity of confidentiality breaches
- Response times for incident investigation and resolution
- Training completion rates and assessment scores
- Audit findings and recommendation implementation
- Staff confidence in confidentiality arrangements
- Service user satisfaction with confidentiality protection

Compliance Activities:

- **Policy Reviews:** Regular review of policies against legal and best practice requirements
- **Process Audits:** Detailed audits of key confidentiality processes and procedures
- **System Testing:** Regular testing of technical security and access controls
- **Documentation Reviews:** Assessment of record keeping and documentation standards
- **Training Assessments:** Evaluation of training effectiveness and knowledge retention
- **External Reviews:** Independent assessment of confidentiality arrangements

Continuous Improvement:

- Analysis of incidents and near-misses for learning opportunities
- Benchmarking against other organisations and best practice standards
- Regular consultation with staff and stakeholders on improvement opportunities
- Implementation of recommendations from audits and reviews
- Investment in new technologies and systems to enhance confidentiality
- Regular policy and procedure updates based on learning and experience

17. REVIEW AND UPDATES

Regular Review Schedule:

- **Annual Policy Review:** Comprehensive annual review of all confidentiality policies
- **Quarterly Performance Review:** Quarterly assessment of confidentiality performance and incidents
- **Monthly Management Review:** Monthly review of confidentiality issues and concerns
- **Incident-Based Review:** Immediate review following serious confidentiality incidents
- **Legal Update Review:** Review triggered by changes in legal or regulatory requirements

Review Process:

1. **Stakeholder Consultation:** Consultation with staff, service users, and external partners
2. **Performance Analysis:** Analysis of confidentiality performance data and metrics
3. **Legal Review:** Assessment of compliance with current legal and regulatory requirements
4. **Best Practice Review:** Comparison with sector best practice and guidance
5. **Risk Assessment:** Review of confidentiality risks and mitigation measures
6. **Recommendation Development:** Development of recommendations for policy improvements
7. **Management Approval:** Senior management review and approval of recommended changes
8. **Implementation Planning:** Development of implementation plans for approved changes
9. **Communication:** Communication of changes to all relevant stakeholders
10. **Monitoring:** Monitoring of implementation and effectiveness of changes

Update Triggers:

- Changes in data protection or confidentiality legislation

- Serious confidentiality incidents or breaches
- Significant changes in organisational structure or services
- External audit recommendations or regulatory requirements
- Professional body guidance or standards updates
- Technology changes affecting confidentiality arrangements

Version Control:

- Clear version numbering and dating of policy documents
- Maintenance of previous versions for reference and audit purposes
- Clear change logs documenting all amendments and reasons
- Distribution lists to ensure all relevant parties receive updates
- Training updates to reflect policy changes

18. CONTACT INFORMATION

Data Protection Officer

- **Name:** Len Chappell
- **Email:** len.chappell@forcesonline.org.uk
- **Phone:** 0300 300 2288
- **Available:** Monday-Friday, 10:00 AM - 4:00 PM

Confidentiality Concerns

- **Email:** len.chappell@forcesonline.org.uk
- **Phone:** 0300 300 2288 (Confidential helpline)
- **Online Contact:** FOL Contacts – Initial Contacts All Sources
- **Via the Veterans VirtualHub:** https://www.virtualhub.uk
- **Online Chat:** Leave contact details with our Chat Heroes service.

Senior Management Team

- **Chief Executive:** len.chappell@forcesonline.org.uk
- **Finance & Estates:** /2IC keith.shields@forcesonline.org.uk
- **HR Manager:** steve.duce@forcesonline.org.uk

- **Chair of the Trustees:** George.dryburgh@forcesonline.org.uk

External Contacts

- **ICO:** 0303 123 1113 / www.ico.org.uk

- **Charity Commission:** 0300 066 9197 / www.gov.uk/charity-commission

---

APPENDIX A: CONFIDENTIALITY AGREEMENT

A copy of the Confidential Staff Agreement can be seen at

https://myfol.uk/staffconfidentialitypolicy.pdf

APPENDIX B: BREACH REPORTING FORM

CONFIDENTIALITY BREACH REPORT

Please use the online form to report breaches.
https://forms.office.com/e/qkTzSsvXWp

Document Control:

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