Privacy and Consent Policy

Operational Guidelines for Client Information Management

1. Purpose

This policy outlines the procedures and requirements for managing client privacy, information sharing, and consent processes to ensure compliance with privacy legislation and best practice standards.

2. Consent Management

2.1 Obtaining Consent

- All clients must sign current consent forms
- Consent forms must be reviewed annually
- Separate consent required for:
  - Information sharing with other services
  - Photographs/recordings
  - Case studies/research
  - Children's information
  - Group work participation

2.2 Consent Validity

- Maximum duration: 12 months
- System alert for expiring consents
- Consent register maintained
- Verbal consent must be documented
- Withdrawal of consent must be recorded immediately

3. Information Sharing

3.1 Need-to-Know Basis

- Information shared only with relevant staff
- Access restricted to necessary information
- Case discussions limited to relevant details
- Team meetings to focus on relevant information
- Corridor conversations prohibited

3.2 External Communications

- Written consent required for external discussions
- Verify identity of external parties
- Document all information shared

- Use client codes in emails
- No client names in email subject lines
- Encrypted email for sensitive information

4. Document Management

4.1 Clean Desk Policy

- All client documents secured when unattended
- Locked filing cabinets for physical files
- Clear desk at day end
- Secure disposal of draft documents
- No client files left in meeting rooms
- Whiteboards cleaned after use

4.2 Digital Security

- Password-protected computers
- Automatic screen locks (5 minutes)
- Secure client management system
- No client information on personal devices
- Encrypted USB drives only
- Regular system backups

5. Email Communications

5.1 Email Standards

- Use client codes instead of names
- No identifying information in subject lines
- Minimum necessary information only
- Check recipients before sending
- Use BCC for group emails
- Double-check attachments

5.2 Email Sanitisation

- Remove identifying details
- Use initials or client codes
- Check metadata in attachments
- Remove location details if unnecessary
- Encrypt sensitive attachments

6. Physical Storage

6.1 Active Files

- Locked filing cabinets
- Restricted access areas
- Sign-out system for files
- No files left unattended
- Regular file audits

6.2 Archived Records

- Secure storage facility
- Access log maintained
- Retention schedules followed
- Secure disposal process
- Annual archive review

7. Electronic Records

7.1 Data Entry

- Accurate and timely recording
- Factual information only
- Professional language
- Regular accuracy checks
- Documentation of sources

7.2 Access Controls

- Role-based access
- Unique login credentials
- Access audit trails
- Regular access review
- Immediate access removal for departing staff

8. Client Rights

8.1 Information Access

- Written request process
- Response timeframes
- Identity verification
- Access restrictions where appropriate
- Appeals process

8.2 Information Correction

- Process for updating information
- Documentation of changes
- Notification of corrections
- Historical record maintenance

9. Breach Management

9.1 Reporting

- Immediate supervisor notification
- Incident report completion
- Client notification if required
- Documentation of response
- Preventive measures identified

9.2 Investigation

- Review of circumstances
- Impact assessment
- Corrective actions
- Policy review
- Staff training needs

10. Staff Responsibilities

10.1 Training

- Annual privacy training
- Procedure updates
- Breach reporting
- Best practice updates
- Competency assessment

10.2 Compliance

- Policy acknowledgment
- Regular audits
- Performance monitoring
- Disciplinary procedures
- Continuous improvement

11. Review and Update

- Annual policy review
- Staff consultation
- Legislative updates
- Incident response review
- Best practice updates

Document Control

Version: 1.0 Date: [Current Date] Review Date: [12 months from current date] Owner: Privacy Officer

Related Documents

- Consent Forms
- Information Release Forms
- Privacy Breach Report Form
- File Access Log
- Archive Register