New Forest Outreach Support C.I.C.

Confidentiality, Data Security & Device Use Policy

Purpose of Policy

New Forest Outreach Support C.I.C. is committed to protecting confidential information, personal data and sensitive records relating to children, families, staff, volunteers and partner agencies.

We recognise that trust, safeguarding and professionalism depend on secure handling of information at all times.

This policy explains expectations regarding confidentiality, secure data handling, device use, access to records and secure disposal of information in line with:

- UK GDPR
- Data Protection Act 2018
- Safeguarding responsibilities
- Professional standards
- Organisational security procedures

This policy applies both on and off organisational premises.

Legal Framework

This policy has been developed in accordance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information Act 2000 (where applicable)
- Children Act 1989 and 2004
- Working Together to Safeguard Children (latest statutory guidance)
- Keeping Children Safe in Education (where applicable)
- Information Commissioner's Office (ICO) guidance

Policy Statement

All confidential information must be:

- Accessed only where there is a legitimate work reason
- Used appropriately and professionally
- Kept accurate and secure
- Shared only where lawful and necessary
- Protected from unauthorised access
- Stored safely
- Disposed of securely
- Collect only the personal information necessary for the purpose it is required.

Every person working for or on behalf of New Forest Outreach Support C.I.C. shares responsibility for protecting confidential information and complying with this policy.

Who This Policy Applies To

This policy applies to:

- Employees
- Directors
- Volunteers
- Apprentices
- Contractors
- Self-employed workers
- Agency staff
- Placement students
- Anyone working on behalf of the organisation

What is Confidential Information?

Confidential information includes, but is not limited to:

- Child records
- Parent / carer details
- Contact information
- Medical information
- SEND information
- Session notes
- Safeguarding records
- Behaviour support plans
- Financial records
- HR records
- Payroll information
- Internal business information
- Emails and correspondence
- Passwords and login information

General Confidentiality Expectations

All staff must:

- Treat information as private and sensitive
- Only access records needed for their role
- Keep discussions professional and discreet
- Never gossip about children, families or colleagues
- Ensure documents are not left visible to unauthorised persons
- Lock screens when devices are unattended
- Use secure passwords
- Report concerns immediately

We Use strong, unique passwords for all organisational accounts and systems.

Where available, enable Multi-Factor Authentication (MFA). Passwords must never be shared, written down where unauthorised persons could access them, or reused across multiple systems.

NFOS administration staff always ensures information is kept accurate and updated where necessary.

Confidential information must never be discussed in public places or casual settings.

Cloud Storage

Electronic records stored within approved cloud systems must only be accessed through authorised organisational accounts.

Files must not be copied into personal cloud storage services or shared outside authorised users without management approval.

Sharing Information

Information may only be shared when:

- There is consent where appropriate
- It is required for safeguarding
- It is necessary for service delivery
- It is required by law
- It is professionally justified and proportionate

Information should only be shared on a need-to-know basis.

Where possible, only relevant information should be shared.

Safeguarding Overrides Confidentiality

Where a child, young person or vulnerable person may be at risk of harm, safeguarding duties override normal confidentiality expectations.

Relevant information may be shared with appropriate agencies such as:

- Children's Services
- Police
- MASH
- LADO
- Health professionals
- Local Authorities

Staff must never promise absolute secrecy where safeguarding concerns exist.

Device Use

Organisation devices remain the property of New Forest Outreach Support C.I.C.

Devices may include:

• Laptops
• Tablets
• Mobile phones
• USB storage devices
• Other electronic systems

All devices must be used responsibly and securely.

Use of Devices Offsite

Devices must not be taken offsite without prior authorisation from management unless this forms part of the role.

Where devices are authorised offsite, staff must ensure:

• Devices remain secure
• Devices are not left unattended in vehicles or public places
• Password protection is active
• Screens are not visible to others
• Information is only accessed where appropriate

Personal Devices

Confidential information must not be downloaded, copied or stored on personal devices unless specifically authorised.

Where exceptional permission is granted, security requirements must be followed.

Remote Working Access

Where remote working is authorised:

- Only approved systems may be used
- Access must be password protected
- Confidential conversations must be private
- Paper records should be avoided where possible
- Information must not be viewed by family members or others

Outreach Access

Staff delivering outreach may access only the information necessary to safely support the child or person they are working with.

Access must be:

- Relevant
- Limited
- Professional
- Time-bound to the support role

When employment or engagement ends, all access must cease immediately.

Data Breaches

A breach may include:

• Lost or stolen device
• Sending information to the wrong person
• Unauthorised viewing of records
• Lost paperwork
• Hacked accounts
• Insecure storage
• Unauthorised sharing

All suspected or actual breaches must be reported immediately to management.

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the organisation will assess the breach promptly and, where legally required, notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach. Individuals affected will also be informed where required by law.

• Information Commissioner’s Office (ICO)
• Local Authority
• Safeguarding agencies
• Other relevant authorities

Visitors

Visitors must not have access to confidential records unless authorised and supervised where appropriate.

Confidential information should not be left visible within meeting rooms or communal areas.

Email Use

Staff must:

- Check recipients carefully before sending confidential information.
- Use organisation email accounts for work-related communication wherever possible.
- Password-protect confidential attachments where appropriate.
- Report misdirected emails immediately.

This is one of the biggest causes of ICO-reportable breaches.

Artificial Intelligence (AI)

Staff must not enter confidential, personal or safeguarding information relating to children, families, staff or organisational business into publicly available AI systems unless authorised by management and appropriate data protection safeguards are in place.

Any approved use of AI must comply with UK GDPR, confidentiality obligations and organisational policies.

This is becoming increasingly common in organisational policies.

Individual Rights

Individuals have rights under UK GDPR including the right to request access to their personal information, request correction of inaccurate information, and, where applicable, request erasure or restriction of processing.

Requests should be referred to the Director as soon as they are received.

Confidential Waste & Secure Disposal

Confidential waste must never be placed in standard bins or recycling.

Examples include:

• Child records
• Printed emails
• Assessment forms
• Incident reports
• Staff records
• Contact lists
• Financial documents

Confidential waste must be:

• Cross-cut shredded, or
• Disposed of through an approved confidential waste provider

Digital information must be:

• Permanently deleted
• Removed from recycle bins
• Removed from shared/cloud systems where appropriate
• Wiped from storage devices before disposal

Storage of Paper Records

Paper records must be:

• Stored securely
• Kept in locked cupboards or offices where appropriate
• Accessible only to authorised persons
• Not removed unnecessarily

Retention of Information

Personal information will only be retained for as long as necessary to meet legal, safeguarding, operational and contractual requirements.

Records will be securely disposed of in accordance with the organisation's Record Retention Schedule once they are no longer required.

Social Media & Messaging

Staff must not use personal messaging apps or social media to share confidential information unless specifically authorised systems are in place.

Photographs or records of children must never be shared through personal accounts.

DISCOVERY Values & Confidentiality

Our confidentiality standards reflect our DISCOVERY values:

D – Dedicated Support
Handling information carefully to keep children safe

I – Individualised Plans
Protecting each child's personal information

S – Specialist Staff
Ensuring trained staff understand confidentiality

C – Child-Led Exploration
Respecting identity, privacy and voice

O – Opportunities for Growth
Creating safe environments built on trust

V – Valued Voices
Helping families feel safe sharing information

E – Empowerment Through Experience
Building trust through responsible practice

R – Respect & Inclusion
Protecting dignity and equality

Y – You Matter
Every child's information matters

Non-Compliance

Failure to follow this policy may result in:

- Informal management action
- Retraining
- Removal of system access
- Formal disciplinary action
- Contract termination
- Legal action where appropriate

Staff Acknowledgement

All staff, contractors and volunteers are expected to read and follow this policy.

Signed acknowledgement may be requested during induction or policy updates.

Monitoring & Review

This policy will be reviewed annually or sooner if required due to:

- Legislative changes
- Data breaches
- Safeguarding updates
- Operational changes
- Lessons learned from incidents

Compliance with this policy may be monitored through supervision, audits, spot checks, incident investigations and system access reviews.