

1. Privacy Notice

1.1. Introduction

NSCM Privacy Notice describes how we use information, particularly information that relates to YP/A.

For employee Privacy Notice please refer to NSCM Employee Handbook.

NSCM is a registered Data Controller with the Information Commissioner's Office (ICO), under registration number Z8473128, for the purpose of collecting and processing personal information.

3.1.1. Data collection

3.1.2. Who do we collect information about?

NSCM collects records and holds information on all YP/A who have been referred for accommodation and/or outreach floating support and have taken up a placement.

We need to know their personal data/information so that we can provide YP/A with the right accommodation and outreach floating support to meet their needs.

3.1.3. What personal data/information do we hold, and why do we collect this information?

Basic personal data/information may be provided to NSCM by the placing authority when they refer a YP/A to NSCM for a service. When contacting us, the YP/A and the referrer will be asked for personal information such as name, address, postcode etc. Information collected to inform the request for a service will include, for example:

- Personal details
- Family details
- Lifestyle and social circumstances
- Financial details
- Employment and education
- Offences and alleged offences

Some information is special due to its sensitivity, it may include:

- Physical or mental health details
- Sex life
- Sexual orientation
- Racial or ethnic origin
- Religious or other beliefs of a similar nature
- Political opinion
- Genetic and biometric data

This might be collected in person, over the phone or via forms sent through secure email or password protected.

Information may also be shared with NSCM by another organisation due to NSCM being part of a package of support being provided. This may include organisations such as national and local NHS bodies, local authorities, police, probation, colleges, and schools.

1.2. Lawful basis

3.2.1. What is the lawful base for NSCM using your personal data/information?

The law on data protection allows NSCM to process, keep or share YP/A's data for certain reasons only.

The information below categorises the type of data processing NSCM undertake and the lawful basis we rely on.

Activity	Lawful basis
NSCM Application form Personal details, special categories, history, lifestyle, social circumstances, risk assessment	Public task
Personal details Name, address, phone numbers, gender, national insurance number, right to work in UK, GP, next of kin, education, financial details, criminal convictions, risk assessment	Public task
Special categories Physical or mental health, disability, sex life, sexual orientation, race, ethnic origin, political opinion, immigration status, religion, genetic and biometric data.	Public task
Risk Assessments Circumstance that may pose a risk to the YP/A or NSCM staff or multi-agency professionals, how to support the YP/A and how to manage the risk.	Public task
Contact sheets. Record of any contact with the YP/A, any professional working with the YP/A, family, or friends, in person, by phone or email.	Public task

<p>Daily / Weekly / Monthly summary report</p> <p>Updates to the placing authority about how the YP/A is getting on in placement, any risks, successes, strengths.</p>	Public task
<p>Accident / incident / injury reports / RIDDOR</p> <p>Accidents and any treatment or hospitalisation, physical or verbal incidences towards NSCM staff or property.</p>	Public task
<p>Safeguarding form or Cause for Concern form</p> <p>Details – reporting a safeguarding or concern to the placing authority, police, or appropriate agencies.</p>	Public task
<p>Missing Person Form</p> <p>If the YP/A goes missing from placement, details of what may have triggered them going missing and risks form is shared with the placing authority, police, or appropriate agencies.</p>	Public task
<p>Independent Living Skills Assessment Form</p> <p>Assessment of how the YP/A getting on living independently.</p>	Public task
<p>Relevant Plans</p> <p>Where the YP/A needs support and what action is required and by whom.</p>	Public task
<p>Permission Form</p> <p>When a YP/A requests NSCM staff speak to an agency on their behalf, or where we may suggest that we can speak to an agency on their behalf.</p>	Contract

1.3. Use of personal data / information

3.3.1. How do we use personal data/information?

NSCM holds personal data/information to enable us to provide appropriate accommodation and outreach floating support packages to YP/A, to refer to specialist services, to maintain our accounts and records.

We may also use information to:

- Deliver services and support to the YP/A.
- Manage services we provide to the YP/A.
- Producing assessments of the health and care needs, child protection or safeguarding.
- Contribute to assessments that may result in the YP/A being taken into care under mental health law, safeguarding or child protection framework.
- Identifying priorities for action.
- Informing decisions on planning of new services.
- Identifying staff training needs.
- Help investigate any worries or complaints to check the quality of the services.

3.3.2. How the law allows us to use the YP/A's personal data/information

We collate and use personal data/information where

- The YP/A or their legal representative have given consent.
- The YP/A have entered an agreement/contract with us.
- To perform our statutory duties.
- To protect someone in an emergency.
- To deliver health and social care services.
- It is required by law.
- To protect public health.

1.4. Information security and data sharing

NSCM is a data controller for the purposes of the General Data Protection Regulation (UK GDPR) January 2021. When processing the YP/A's personal information we will aim to do so fairly, lawfully and in line with the UK GDPR. Information will not be held for longer than required and will be disposed of securely.

We will work in an open and transparent way, discussing and/or sharing any reports, updates and assessments written by the outreach worker, with the YP/A, before sending them to the placing authority.

We will only share the YP/A's personal data/information after discussions with them, with appropriate organisations such as the NHS, health care professionals, social care, and welfare organisations. The Care Quality Commission and/or Ofsted may also request access to information as part of an inspection or monitoring process of NSCM. We will only share personal data/information once the necessary legal basis has been established and data protection safeguards have been verified. See Lawful basis above.

We will not give or sell YP/A's information to any third party for marketing purposes.

1.5. Rights of young people / adults

3.5.1. What are the rights of the YP/A?

YP/A have the right to ask for all the information we have about them. When we receive a request from a YP/A in writing, we must give them access to everything that we have recorded about them. If the YP/A cannot request this in writing, they should speak to their outreach worker who will need to consider another way to enable the YP/A to make this request.

However, we are unable to let YP/A see any information held in their records which contain confidential information about other people or where a professional thinks this will cause serious harm to the YP/A or someone else.

3.5.2. 'Right to be forgotten' – you can ask for information to be deleted.

In some circumstances YP/A can ask for their personal data/information to be deleted. For example, where there is no legal reason for us to use it. If a YP/A believes the information we hold is wrong, they have the right to have it corrected or deleted.

Information required by law cannot be deleted where it is used for public health purposes or if it is necessary for legal claims.

3.5.3. Limit the use of your personal data / information.

YP/A can request for NSCM to restrict what we use their personal data/information for and where they have identified inaccurate information and have told us about it.

Where possible NSCM will seek to comply but may not be able to where we need to hold or use the YP/A's information because we are required to by law.

3.6. Protecting personal data / information

3.6.1. How we protect the YP/A's personal data/information

We hold all records about the YP/A (paper or electronically) securely and only make them available to those who have the right to see them.

We secure information by using secure emails; hiding parts of your personal information from view and password protect electronic documents.

We ensure that emails are sent without revealing addresses to other recipients and use blind carbon copy (bcc), not carbon copy (cc). We also check group email addresses and only send the message to the people that need to see it.

Paper documents are held in a secure cabinet and locked room/office.

Paper is shredded and disposed of securely.

NSCM mobile phones and devices used by staff in the course of their work with you are password protected.

3.6.2. How we keep NSCM safe and protect against online risks

NSCM IT equipment has firewalls and virus checking systems to protect your personal data/information. Staff working for or on behalf of NSCM are expected to protect their personal devices i.e., mobile phones/IT equipment, if used for NSCM business.

All devices/IT equipment are password protected; in addition, all files containing personal data/information held on this equipment are password protected.

NSCM take the following actions to minimise the risk of personal data/information being compromised.

- Train staff.
- Staff declaration and commitment to reporting data breach.
- Email disclaimer.
- Secure email and file transfer.
- Delete suspicious emails.
- Robust reporting mechanisms in the event of lost or stolen devices (laptops, iPads, tablets, mobile phones etc).
- Strong password protection on all devices.
- Download software updates.
- Use of anti-virus software.
- Decommissioning the removal of data from devices/hardware no longer in use or obsolete.
- Memory sticks password protected.
- Refresh NSCM Policy & Procedures and continue to review the procedures annually.

NSCM have an encrypted backup storage server / system. The backup system stores information on the cloud and is backed up each night. This system is encrypted to protect all stored data/information.

NSCM rely on Egress Switch secure email and file transfer to communicate and share information and need to protect the personally and commercially sensitive data that staff share both internally and with external users. Egress Switch secure email and file transfer provides easy-to-use, flexible email and file encryption that offers the highest levels of security and access controls, in addition to encrypting message content and attachments. Switch secure email and file transfer provides total control over shared information in real time, with the ability to revoke access, audit user actions and add message restrictions to prevent data mishandling.

3.7. Standards

- Government and industry-certified

- Switch secure email and file transfer features comprehensive government and industry-certified security and authentication, including email and file encryption at rest and in transit, multi-factor authentication, and customisable policy controls.
- Users can stay in control of their information after it has been shared both internally and externally by revoking recipient access, preventing actions such as download and copy/paste, and viewing audit logs.
- Switch is certified under NCSC Commercial Product Assurance, Common Criteria, and ISO 27001:2013

3.8. Keeping personal data/information

3.8.1. How long do we keep YP/A's personal data/information for?

We are required, by law, to keep care YP/A's personal information for a set period of time and this can range from months to decades for more sensitive records.

Records for YP/A leaving care are retained from the date of birth +75 years or 15 years after death of child (where child dies under 18). Adults with mental health difficulties and/or subject to the Mental Health Act files are retained from the last action +20 years. The only reason this may differ is if a local authority advises otherwise.

3.9. Concerns

3.9.1. If YP/A has concerns about how we use their personal information.

YP/A can make a complaint if they have a concern about the way NSCM is handling their information, they should email info@nscm.co.uk or they can complete an NSCM Complaint/Compliment form which can be downloaded from www.nscm.co.uk or they can contact NSCM Director of Finance and Compliance, Philip Savva on Tel: 0208 211 3663. The Director of Finance and Compliance will liaise with the RSM who will investigate your complaint and respond within 15 working days.

If that response does not fully address the YP/A's complaint, or if they are still not satisfied with our actions, they can contact the Information Commissioner's Office ('ICO'). The ICO is an independent official appointed to oversee the UK General Data Protection Regulations, January 2021. Further information can be found on the ICO website <https://ico.org.uk>. The ICO's address is Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF and the phone number is 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.