

THE NATIONAL MINIMUM DATA SET FOR SOCIAL CARE (NMDS-SC)

FAIR PROCESSING NOTICE : LAYER 3

CONTENTS

1.	INTRODUCTION TO THE NMDS-SC	3
2.	PURPOSE OF THIS FAIR PROCESSING NOTICE	4
3.	INFORMATION COLLECTED IN THE NMDS-SC.....	5
3.1	REASON FOR COLLECTING DATE OF BIRTH	5
3.2	REASON FOR COLLECTING THE NATIONAL INSURANCE NUMBER (NINO)	5
3.2.1	<i>Permission obtained from NINO Board</i>	<i>5</i>
3.3	REASON FOR COLLECTING GENDER	6
3.4	REASON FOR COLLECTING HOME POSTCODE	6
3.5	REASON FOR COLLECTING ETHNICITY AND DISABILITY STATUS.....	6
4.	COMPLIANCE WITH THE DATA PROTECTION ACT 1998.....	7
4.1	STATUS AS DATA CONTROLLERS IN COMMON.....	7
4.2	FAIR PROCESSING OF PERSONAL AND SENSITIVE PERSONAL DATA	7
4.2.1	<i>The Data Protection Act 1998 Schedule 2 and Schedule 3 Fair Processing Conditions</i>	<i>7</i>
4.2.2	<i>Employers' fair processing obligations and completion of the NMDS-SC.....</i>	<i>8</i>
5.	ACCESS TO INFORMATION	10
5.1	PARENT ORGANISATIONS	10
5.2	CSCI AND GSCC.....	10
5.3	SUBJECT ACCESS REQUEST.....	10
5.4	FREEDOM OF INFORMATION ACCESS REQUEST.....	11
5.5	RELEASE OF 3RD PARTY INFORMATION	11
5.6	STATUTORY RELEASE OF DATA.....	11
5.7	SECONDARY USE OF DATA	11
6.	ACCESS CONTROLS AND AUTHENTICATION.....	12
7.	SYSTEM SECURITY	13
7.1	BUSINESS CONTINUITY AND DISASTER RECOVERY	13
7.2	TRAINING.....	13
7.3	MONITORING OF SECURITY INCIDENTS	14
7.4	BREACH OF SECURITY INCLUDING BREACH OF CONFIDENTIALITY	14
8.	CHANGE CONTROL.....	14
9.	RETENTION OF DATA.....	14
10.	GENERAL	15
10.1	CONFIDENTIALITY	15
10.2	DATA INTEGRITY	15
10.3	INDEMNITY	15
11.	APPENDIX A: RELEVANT LEGISLATION	16
11.1	DATA PROTECTION ACT 1998.....	16
11.1.1	<i>Definition of sensitive personal data.....</i>	<i>17</i>

11.1.2	<i>Schedule 2 : processing of personal data</i>	17
11.1.3	<i>Schedule 3: processing of sensitive personal data</i>	17
11.2	FREEDOM OF INFORMATION ACT 2000	19
11.3	DATA PROTECTION AND FREEDOM OF INFORMATION – HOW DO THE TWO INTERACT?.....	20
11.4	THE INFORMATION COMMISSIONER.....	20
11.5	COMPUTER MISUSE ACT (1990)	20
12.	APPENDIX B – GLOSSARY OF TERMS	21
13.	APPENDIX C – NMDS-SC DATA ITEMS	23
14.	APPENDIX D: NMDS-SC ONLINE SYSTEM CONTRACTUAL PROVISIONS	25

1. INTRODUCTION TO THE NMDS-SC

The National Minimum Data Set for Social Care (NMDS-SC) is a system for collecting and analysing information about the social care workforce in England. Accurate workforce data on the entire social care sector in England is needed in order to:

- reduce vacancy rates and encourage new entrants,
- improve recruitment and retention rates,
- increase numbers of staff with relevant qualifications and skills and
- modernise the workforce

to meet society's future needs for social care.

The NMDS-SC is operated by Skills for Care. Skills for Care is the national workforce development organisation for adult social care in England, and is part of the sector skills council Skills for Care & Development.

Skills for Care

Albion Court, 5 Albion Place, Leeds LS1 6JL, United Kingdom

Telephone: 0113 245 1716 Website: www.skillsforcare.org.uk

Registered Charity 1079836. Registered Company 3866683. VAT No 853 0479 22

Data Protection Act 1998 Data Controller registration no. Z6220820

NMDS-SC Help Line: 0845 873 0129 or nmds@skillsforcare.org.uk

The NMDS-SC was developed in 2004-5 by Skills for Care working in partnership with the Department of Health, the Department for Education & Skills¹, the General Social Care Council (GSCC), the Commission for Social Care Inspection (CSCI), the Social Care Institute for Excellence (SCIE), NHS National Workforce Projects, the Local Government Association (LGA), the Learning & Skills Council (LSC) and other key stakeholders.

The NMDS-SC was launched in October 2005 and information was collected from social care employers under interim arrangements via an Excel spreadsheet and paper questionnaires. The NMDS-SC Online system, which enables social care employers to complete the NMDS-SC online, was launched in November 2007. Employers who do not have access to the Internet may continue to complete paper questionnaires and the data they provide is entered into NMDS-SC Online by Skills for Care on their behalf.

Private and voluntary sector organisations, local authorities and other employers of social care workers including the NHS and individuals employing their own care and support workers are being asked to provide information about their services and staff into NMDS-SC Online. See Appendix C for the data items collected by the NMDS-SC.

The system can be accessed via a website www.nmds-sc-online.org.uk. Once registered on the system, employers can access their own data. Aggregated data on comparable services is freely available for analysis, comparison and planning but is always anonymised so that other employers and commissioners cannot identify individual employers.

Employers can input into NMDS-SC Online and update their organisational and staff details as frequently as they wish. The more up to date the information is within the system, the more accurate and timely the reports produced by the system are.

Completion of the NMDS-SC is not mandatory and all data are submitted voluntarily by employers.

¹ Now the Department for Children, Schools & Families.

2. PURPOSE OF THIS FAIR PROCESSING NOTICE

This notice aims to outline the information governance arrangements in place for the NMDS-SC, and to provide assurance to employers that the information they provide is held in a safe and secure environment and is compliant with key legislation. The key legislation this document refers to is:

- The Data Protection Act 1998 (DPA)
- The Freedom of Information Act 2000 (FOIA)
- The Computer Misuse Act 1990.

All employers signing up to access and use the NMDS-SC Online system agree to comply with the Data Protection Act 1998, the Freedom of Information Act 2000, the Computer Misuse Act 1990 and any other legislation deemed appropriate.

This document relates to specific risk areas to both employers and Skills for Care, aiming to mitigate such risks wherever possible. For detailed information regarding the aforementioned legislation please refer to Appendix A.

The rules, guidance and procedures described within this document prescribe the agreed procedural and security controls for Skills for Care and employers with regard to distribution and protection of information within the NMDS-SC Online system, and aim to ensure that:

- The system is appropriately assessed for compliance with industry standard security requirements.
- Availability of the system is ensured (information is delivered to the right people, at the right time and in compliance with the organisation's business objectives).
- Integrity is maintained (the system operating correctly according to specification, protected from unauthorised or accidental modification, and ensuring accuracy and completeness of the organisation's data).
- Confidentiality is preserved against unauthorised disclosure.
- Accountability is enforced (staff are made aware of and held to account for their roles and responsibilities in regard to security).
- Breaches of security are detected and resolved.

3. INFORMATION COLLECTED IN THE NMDS-SC

The NMDS-SC is collected at establishment, i.e. individual workplace, level (see Appendix B for definition of an establishment).

The NMDS-SC dataset is in two parts:

1. information about the establishment (“organisational data”)
2. information about each worker (“worker data”)

The organisational data includes contact details, legal status of business, Investors in People status, services provided, total workforce, starters, leavers and vacancies.

The worker data includes gender, date of birth, National Insurance Number, ethnic group, disability status, job role, pay, hours worked, qualifications. Individuals’ names, addresses and contact details are **not** collected.

For a full list of organisational and worker data items please refer to Appendix C.

Under the Data Protection Act 1998, the information about workers is defined as personal data. The reasons for collecting specific data about workers are outlined below:

3.1 Reason for collecting date of birth

Date of birth is collected for two reasons: to calculate workers’ ages, an important piece of information for workforce planning, and to create a unique reference number for each worker (see also Section 3.2).

3.2 Reason for collecting the National Insurance Number (NINO)

One of the main tasks of the NMDS-SC is to measure how many people work at different care providers at the same time, and how workers move into, within and out of the social care workforce. This is very important for understanding the extent to which social care depends on people doing more than one job, and the number of people that will need to be employed in social care in future.

To do this the NMDS-SC needs to be able to **distinguish between individual workers**. In the NMDS-SC system, this is achieved by an automated process which creates a *unique reference number* for each worker, by combining and encrypting their National Insurance Number (NINO) and date of birth. This is necessary as the NINO alone may not be unique - a few national insurance numbers are duplicated.

However, the NMDS-SC does not seek to know the identity of these workers, and their names and addresses are consequently **not** collected. The distinction between **distinguishing** between workers and **identifying** them is important, and it should be emphasised that the NMDS-SC is not designed to do the latter.

3.2.1 Permission obtained from NINO Board

At the outset of the NMDS-SC project Skills for Care sought permission from the Department of Work & Pensions NINO Board to collect and use the NINO for the purpose of internal data matching only, and not linking to any data which could directly identify individuals.

After considering the Skills for Care proposal, the NINO Board were satisfied that this particular proposal did fall within the context for which a NINO could be used. The NINO Board therefore approved on 23 August 2005 the use of the NINO for those purposes as specified by Skills for Care, subject to the following caveat:

Skills for Care Ltd. are fully responsible for ensuring compliance with the Data Protection Act. The Office of the Information Commissioner would need to advise on any specific data protection issues relating to sharing information.

The approval of the NINO Board has no time limit.

All analysis, reporting and output of worker data from the NMDS-SC is conducted using the unique reference number and not the NINO. Once the unique reference number is created, the NINO can only be retrieved from it by running decryption algorithms only available to technical staff at Skills for Care’ trusted IT partner Tribal Education Ltd.

3.3 Reason for collecting gender

Social care is heavily reliant upon female workers, and therefore gender is important information for workforce planning and for establishing the extent to which male workers are being attracted into the workforce.

3.4 Reason for collecting home postcode

The home postcode is collected solely to calculate the distance travelled to and from work, by calculating the distance between home and work postcodes using standard software. How far workers of different types are prepared to travel to work is key information for workforce planning, especially in rural areas.

Under no circumstances is home postcode used to identify individual workers' addresses.

3.5 Reason for collecting ethnicity and disability status

Government policy is for the social care workforce to reflect the culture and diversity of the local area it serves. Ethnicity and disability status is therefore important information for workforce planning and for monitoring the effectiveness of programmes to recruit a wider range of people into social care.

In particular, information on the extent to which disabled people are working across the range of social care services is currently very limited, and greater knowledge is required to help target resources and inform future recruitment initiatives.

Under the Data Protection Act 1998 ethnicity and health-related data are classed as **sensitive personal data** (see glossary and next section).

4. COMPLIANCE WITH THE DATA PROTECTION ACT 1998

As the NMDS-SC data collected includes both personal data and sensitive personal data, the Data Protection Act 1998 requires certain conditions to be met for the data to be processed lawfully.

4.1 Status as Data Controllers in Common

Prior to the development of the NMDS-SC Online system, Skills for Care approached the Information Commissioner's Office². It was agreed that, with reference to their respective responsibilities under the Data Protection Act, the Employer (legal entity) and Skills for Care are **Data Controllers in Common**. This means that both parties share a pool of personal data, each processing independently of the other.

To reflect this, organisations providing data to the NMDS-SC should if necessary update their data protection registration with the Information Commissioner's Office.

Skills for Care's registration, which outlines the purpose for which data are to be used, can be viewed at www.ico.gov.uk/tools_and_resources/register_of_data_controllers.aspx

It is the responsibility of each employer whose worker data are provided to the NMDS-SC Online system to ensure that it complies with the Data Protection Act 1998.

4.2 Fair processing of personal and sensitive personal data

As Data Controllers in Common, employers providing information about their workers to NMDS-SC Online need to meet the fair processing conditions laid out in Schedules 2 and 3 of the Data Protection Act 1998. These are summarised below; for details see Appendix A or the text of the Data Protection Act 1998 at www.opsi.gov.uk/acts/acts1998/19980029.htm

4.2.1 The Data Protection Act 1998 Schedule 2 and Schedule 3 Fair Processing Conditions

In order to comply with the Data Protection Act when processing personal information, certain fair processing conditions must be met.

First of all, the type of data being processed needs to be established: personal data or sensitive personal data.

Personal Data means data relating to a living individual who can be identified from those data (including opinion and expression of intention).

Sensitive Personal Data means data concerning ethnicity, disability, health, sexuality, offending etc. (see Appendix A for detailed definition).

For the purpose of the NMDS-SC the "worker data" are **personal data**. However two of the data items are **sensitive personal data** – ethnicity and disability. In order to comply with the Act:

- when processing **personal data** one condition in Schedule 2 must be met for the data to be considered fairly processed.
- for processing **sensitive personal data** one condition in Schedule 2 and a condition in Schedule 3 should also be met for the data to be considered fairly processed.

The conditions under which personal and sensitive personal data can be processed fairly under the Data Protection Act 1998 are summarised below. This is only a summary - for a full explanation please refer to Appendix A or to the full Data Protection Act (1998) at www.opsi.gov.uk/acts/acts1998/19980029.htm

Schedule 2: Personal data processing conditions

The data subject has given consent to the processing,

Or

The processing is necessary for:

2. A contract
3. Other legal obligation

² See Appendix A for explanation of role of the Information Commissioner.

4. Protection of the vital interests of the data subject
5. Exercise of justice, a statutory obligation or other public function, or in the public interest
6. Legitimate interests of the Data Controller

Schedule 3: Sensitive personal data processing conditions

The data subject has given explicit consent to the processing,

Or

The processing is necessary for:

2. Employment related purposes
3. Protection of vital interests of the individual (where consent cannot be obtained)
4. Membership of bodies or associations
5. Made public by the data subject
6. Legal proceedings
7. Administration of justice or statutory functions
8. Medical purposes
9. Equalities and diversity monitoring

The condition under which **personal data** are being processed fairly by Skills for Care is Condition 6: Legitimate interests of the Data Controller.

The conditions under which **sensitive personal data** are being processed fairly by Skills for Care are, in addition, Condition 2: Employment related purposes and Condition 9: Equalities and diversity monitoring.

4.2.2 Employers' fair processing obligations and completion of the NMDS-SC

Employers should take a view about their obligations under the Data Protection Act 1998 with regard to the fair processing of their workers' personal information and sensitive personal information supplied to NMDS-SC Online.

If an employer feels that the processing for NMDS-SC Online meets the necessary conditions set out above, then neither consent (for personal data) and/or explicit consent (for sensitive personal data) need be sought.

However, if an employer feels that, to meet the fair processing conditions, the consent of each worker should be obtained before providing any sensitive personal information, or any personal information at all, to NMDS-SC Online, it will be necessary to achieve:

- Consent for providing personal information. Consent can be defined as '*any freely given specific and informed indication of wishes and which the data subject (i.e. worker) signifies his/her wishes*'. An employer needs to be confident that there has been '*active communication*' with these workers about the contents of the NMDS-SC and that these workers consent to this information being provided.
- Consent for providing sensitive personal information. This needs to be '*explicit*' and '*absolutely clear*'. The worker's (data subject's) consent must be clear and cover items such as the specific details of processing, the data to be processed and the purpose for processing.

There are two ways to achieve consent:

1. Opting-in: where workers are invited to give permission for their individual data to be included onto the NMDS-SC system. Opting-in is a demonstrably clear way of gaining consent. It is the employer's responsibility to ensure that each worker is made fully aware of what the data are to be used for and by whom. If an employer feels that it is the most appropriate way to obtain consent that is '*explicit*' and '*absolutely clear*', in order to complete all the items in the NMDS-SC including the two sensitive personal items (i.e. ethnicity and disability) then consent must be signified by some communication between the employer and the worker (data subject). If the data subject does not respond this cannot be assumed as implied consent. (For definition of a data subject please refer to Appendix B Glossary of Terms).

2. Opting-out: where workers are invited to inform their employer if they wish their individual data to be withheld from this system. When opting out, workers can choose not to have all or specific data items provided. Employers using this approach must be confident that there is active communication with staff regarding the purpose and use of the information stored within the NMDS-SC system, specifically including the two sensitive personal items. A worker can opt out of sharing part or all of their personal and personal sensitive data. This approach assumes implied consent if a worker does not respond.

Employers need to advise their workers that they will, through the completion of NMDS-SC Online or via paper questionnaire for entry into Online, be providing data to Skills for Care.

Each individual worker has the right to request that their details in full or part are not submitted to NMDS-SC Online. It is the responsibility of the employer to establish and manage consent. If consent is sought, each worker (data subject) must have the right to withdraw consent. It is the responsibility of the employer to inform workers of this right, and to implement any removal of worker's consent.

An employer can withdraw from the NMDS-SC system at any time and an individual worker can remove their consent at any given time. This will be effective immediately, with the current record being removed. However, historical aggregated NMDS-SC data used for analytical purposes is retained and any removal of data is not retrospective in nature (see Section 9 Retention of Data).

5. ACCESS TO INFORMATION

All NMDS-SC data are held securely, in accordance with the Data Protection Act 1998, on a system owned by Skills for Care. The system is managed and supported on a day-to-day basis by Skills for Care's contractual IT partner Tribal Education Ltd, which operates the system in compliance with the Data Protection Act 1998. For a summary of the contractual provisions governing the operation of the system, please see Appendix D (to follow).

Skills for Care is committed to keeping all personal data safe and secure and will not pass individuals' personal data to any third party unless employer permission has been given or unless it is legally obliged to do so.

Access to detailed employer and worker data obtained either via NMDS-SC Online or via paper or Excel questionnaires is only available to the following trusted parties:

1. The employer who submitted the data,
2. The parent organisation (if applicable, and if permission has been given by the employer; see below for an explanation of parent-establishment relationships and responsibilities),
3. A small number of key Skills for Care business support staff who are responsible for assisting establishments and administering the NMDS-SC, and
4. A small number of key staff at Tribal Education Ltd who are responsible for technical system management and support.

5.1 Parent organisations

In the NMDS-SC Online system, employers whose establishments are part of a larger organisation can choose whether they or their parent organisation is the "owner" of the establishment's data. The "owner" of the establishment has permission to access, view and update the establishment's worker data. If the parent is the "owner" then only the parent employer may access, view and edit the establishment's worker data. If the establishment is the "owner" then only the establishment employer may access, view and edit its worker data.

The "owner" can specify whether it allows the "non-owner" to access and view, but not edit, the worker data. Thus if the parent organisation is the "owner" it can give permission to the establishment to access and view individual worker data, and if the establishment is the "owner" it can give permission to the parent to access and view individual worker data.

It is the responsibility of the "owner" to ensure that these relationships are specified and operated in conformity with the Data Protection Act 1998 and other relevant legislation.

5.2 CSCI and GSCC

Under current arrangements, employers in establishments registered with the Commission for Social Care Inspection (CSCI) may choose to provide some of their NMDS-SC data to the CSCI as part of the Annual Quality Assurance Assessment (AQAA) return. Employers choosing to do this may do so by downloading from the NMDS-SC Online system a completed version of the workforce section of their AQAA return and sending it, together with the rest of their AQAA return, to the appropriate regional CSCI office.

In future, it is anticipated that employers may be able to provide their data to the General Social Care Council (GSCC) as part of their worker registration requirements, via a similar process.

Also in future, it is intended that, for establishments registered with the CSCI/its successor body and only if permission has been granted by the employer, some of the personal and sensitive personal information provided to the NMDS-SC may be shared with CSCI/its successor body as input to the AQAA. This facility is not available at present. The employer may choose not to share these data with CSCI/its successor body.

5.3 Subject Access Request

The Data Protection Act 1998 gives data subjects a general right of access to personal information which relates to them, as defined in Section 7, 8 and 9 of the Act.

All subject access requests for data from the system will be dealt with by the Data Controller receiving the request. This will either be the data subject's employer or Skills for Care.

All requests for information will be dealt with in compliance with the Data Protection Act 1998, and will be processed within 40 days on receipt of the required fee and the necessary information to confirm the identity of the data subject. The Data Controller may charge a fee of up to £10 for providing the data subject with the information requested.

5.4 Freedom of Information Access Request

All Freedom of Information requests made to Skills for Care will be processed and actioned in accordance with the Act. In order to comply with the Freedom of Information Act 2000 Skills for Care is not required to seek an establishment's permission to release information if requested to do so under the Act. Information released will comply with relevant legislation, using exemption as appropriate, such as not releasing personal or commercially sensitive information.

All Freedom of Information requests will be dealt with within 40 days on receipt of the required fee and the necessary information to locate the data. The Data Controller may charge a fee of up to £10 for providing the information requested.

5.5 Release of 3rd Party Information

Unless a legal obligation is identified for Skills for Care to do so, no personal information provided to Skills for Care as data processors will be given to any other party nor will it be used for any other purpose than detailed in this Fair Processing Notice without informing and obtaining the consent of the original provider.

5.6 Statutory Release of Data

Where Skills for Care has a statutory obligation to disclose personal information then the consent of the data subject is not required, but the data subject should be informed that such an obligation exists. An example of this would be under a FOI request or a criminal investigation.

5.7 Secondary Use of Data

There is a range of standard and ad-hoc outputs from the NMDS-SC Online data warehouse, available at different geographical levels and downloadable in Excel spreadsheets, other electronic formats and printed versions. These include (but are not limited to):

Establishment-level Reports of individual employing organisations, for individual employers to use for their own HR development and workforce planning purposes, for submission to CSCI, local authorities and other bodies as employers see fit, and, with permission from the employer, to support the work of:

- Skills for Care Regional Offices, for training needs analysis and to release funding for local training requirements;
- Skills for Care Social Work Development Partnership (former Learning Resource Network), to identify learning opportunities.

Worker Reports on individual workers, for employer's own use.

Standardised Statistical Reports of aggregated data at national, regional and sub-regional level, providing analyses at regular intervals in the form of tables, charts and graphs and with statistical measures such as means, medians etc., for workforce planning and policy development.

Ad-hoc Analyses of aggregated national, regional and sub-regional data, performed on request by Skills for Care analysts.

Data Downloads whereby aggregated national, regional and sub-regional data in standard formats, e.g. CSV files can be exported for analytical use by researchers and other users in applications such as SPSS, Excel and other analysis software, and to add to other databases using standard labels e.g. date, postcode.

6. ACCESS CONTROLS AND AUTHENTICATION

Access controls are fundamental to the security of all computer systems, and to achieve compliance with the Data Protection Act 1998. NMDS-SC Online has the following access controls and authentication systems:

Password control: all passwords must be at least 6 characters long; at least one must be a letter and at least one must be a number.

Security question: the system will ask the user to provide a security question and answer of their choice. The purpose of the security question is to allow Skills for Care business support staff to authenticate users who have been locked out of their account, thus allowing their account to be re-activated. The security question and answer is available to Skills for Care business support staff.

Interim Solution Employers: Skills for Care contacted via letter all employers who provided NMDS-SC data prior to February 2008 under interim solution arrangements (i.e. collection of data via paper or Excel questionnaires). The letter included user name and password providing the employer with access to the NMDS-SC Online system into which their data had been migrated. Upon accessing the system for the first time, users were required to add the establishment's NMDS-SC ID number and provide a valid e-mail address. An automated security e-mail was then sent from the system to the user with instructions for completion of the registration process.

New employers: NMDS-SC Online is available via the Internet to employers who can register and input information online. In support of social care employers who do not have access to the Internet, Skills for Care continues to accept paper based submissions, which are managed by Skills for Care staff of behalf of the employer and entered into NMDS-SC Online.

Registration: All employers registering with NMDS-SC Online are for security reasons manually validated by Skills for Care staff. This is generally done via publicly-accessible sources: CSCI or Ofsted registration, BT listings, internet searches, contact with commissioning authorities and other methods. Employers may be contacted directly to find out more about the services they provide. Each employer registered with NMDS-SC Online has a maximum allocation of three user accounts, thus allowing up to three separate named staff to administer their data via the system. This is to prevent password sharing and to allow auditing of any amendments, deletions or creation of records. Upon login a user is informed of the time and date of the last login. Any unauthorised or fraudulent use of user accounts should be reported to the NMDS-SC Online Help Desk.

User profiles: The table below identifies the roles available on the system and the level of information each has access to. See Appendix C for a full list of organisational and worker data items.

User Profile	Role Based Access	Aggregated data	Individual Establishment data	Individual worker data
Employer User (Establishment level; up to 3 users per Establishment)	To be agreed within each organisation	YES	YES	YES
Parent Employer	Only by appropriate authorisation from the Employer (Establishment level) and Skills for Care	YES	YES	YES
Administrator	Skills for Care Help Desk and Business Support staff, and Tribal Education Ltd technical staff	YES	YES	YES
Root User	Skills for Care and Tribal Education Ltd access for maintenance	YES	YES	YES

User Profile	Role Based Access	Aggregated data	Individual Establishment data	Individual worker data
	and system development. Also to create admin user accounts.			
Skills for Care Regional NMDS-SC Lead	Only by appropriate authorisation from the establishment and Skills for Care	YES	YES	NO
All other Skills for Care staff, plus all external organisations e.g. Department of Health, other government departments, researchers		YES	NO	NO

7. SYSTEM SECURITY

NMDS-SC Online uses SSL (Secure Sockets Layer) cryptographic protocol technology to provide secure communications via the internet. This is a robust and trusted solution used for many internet banking, e-commerce, secure e-mail systems etc. and have been endorsed by financial organisations such as Visa, Mastercard and American Express. The technology utilises industry standard 128-bit encryption.

To verify the security of NMDS-SC Online Skills for Care have carried out an initial 'penetration testing' of applications, technical infrastructure and Help Desk business processes using an independent third party agency. Skills for Care will continuously monitor and evaluate security related issues to ensure the integrity of NMDS-SC data and systems.

Responsibility for system operation, maintenance and development resides within Skills for Care and is supported by the contractual agreement with Tribal Education Ltd. Users who require assistance in relation to NMDS-SC Online, or who experience performance or functionality problems when using the system should contact Skills for Care via the NMDS-SC Help Desk. System performance is monitored on an ongoing basis in consultation with users. This process is documented in the Service Schedules.

7.1 Business Continuity and Disaster Recovery

Skills for Care and its contractor Tribal Education Ltd have implemented an agreed procedure regarding system down time. Skills for Care will ensure that warnings are given to all system users regarding any planned downtime and also to provide advice and guidance during any unscheduled downtime. Notices regarding down time will primarily be communicated via the NMDS-SC Online website.

Disaster Recovery (DR) processes are also in place for NMDS-SC Online to ensure continuous service in relation to applications, technical infrastructure and Help Desk processes in case of serious and/or catastrophic failure. A formal DR review will be held annually to assess risks and evaluate implications of failure to system.

7.2 Training

Users may request training in system use, security and confidentiality issues in advance of receiving access to the live system. Training is provided by Skills for Care or any of its affiliated partners and should be requested by contacting the NMDS-SC Online Help Desk.

7.3 Monitoring of security incidents

A security incident is defined as the attempted or successful unauthorised access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. If an incident of this nature detected by an employer it should be reported in line with the organisation's own security procedures. These can often be found in the Organisation's Security Policy. Breach of security protocols by an organisation's own employee(s) should be reviewed by the organisation's Information Security representatives in line with their existing procedures and reported to Skills for Care.

In case the data of other organisations are put at risk following an incident/breach by one organisation, only general information regarding the incident/breach will be divulged – no organisational or personal data will be disclosed.

Security advice resulting from the investigation of incidents will be reviewed and agreed by Skills for Care and the supplier and shared with users of the NMDS-SC Online system as appropriate.

7.4 Breach of Security including breach of confidentiality

Each establishment is responsible for investigating any reported breaches by its own staff and taking appropriate disciplinary action where necessary. Skills for Care and Tribal Education Ltd will be responsible for investigating any reported breaches by their own staff.

Skills for Care has to right to suspend and revoke access to any employer or individual user if inappropriate usage is suspected. Following an investigation, the employer and Skills for Care will agree on an appropriate action. If either party is unhappy with the action undertaken then both organisations should seek an independent opinion.

8. CHANGE CONTROL

Procedures are in place for the management of changes to NMDS-SC and the NMDS-SC Online system, and are documented in the NMDS-SC Change Management Policy and Procedure. The document sets out the process for change management relating to both technical/system areas and to NMDS-SC data items. Changes should be requested on the formal Request For Change form and submitted to Skills for Care for processing. Skills for Care is responsible for undertaking the testing and acceptance of any implemented changes. System users will not be engaged in this process unless deemed necessary by Skills for Care.

9. RETENTION OF DATA

Employer level data are held on the system until deleted by the employer or by Skills for Care if requested to delete data on behalf of the employer.

If a worker leaves the organisation, the employer should upon their next update remove the individual's data from the system. If an individual requests his/her data to be removed from the system, the employer should remove the data forthwith. Once an individual or an employer is deleted from the system the relevant data are removed from the operational (live) database and are no longer available. However, data are still held within database 'audit tables', a feature which allows for database transaction tracking and monitoring. Complete removal of employer/worker data from the system (i.e. from the operational database including the audit tables) can be carried out on request from the employer/individual.

Analytical "snapshots" of the operational database containing anonymised data for analysis/research purposes are produced at the end of every month for the NMDS-SC Online data warehouse. Such data are essential to the development and operation of the NMDS-SC as a source of historical workforce data on the social care sector in England, and are retained indefinitely. In the long term, it is intended that historical NMDS-SC data will be stored in the Social Sciences Archive at the University of Essex.

Reports produced from the operational database will not be saved by the system. Users are therefore recommended to download and save on their local systems any reports required for future use.

10. GENERAL

10.1 Confidentiality

To prevent the identification of any individual of whom there are a small number within an organisation, e.g. Registered Managers, all employee numbers below a certain 5 are suppressed. This is to maintain confidentiality and to minimise the risk of individual workers being identified.

10.2 Data Integrity

Skills for Care accepts no responsibility regarding the data quality or integrity of data held within the system. Responsibility for an employer's data lies solely with the employer.

10.3 Indemnity

Where any breaches of security or legislation occur and result in legal proceedings against an organisation holding Data Controller or Data Processor for NMDS-SC data, responsibility and liability will be jointly discussed and agreed. As Data Controllers in common both the employer and Skills for Care are legally responsible for the data held within the NMDS-SC Online system. If any disclosure was proven to be as a result of a technical fault or neglect then Skills for Care and Tribal Education Ltd would engage in the review process and accept liability if deemed appropriate.

11. APPENDIX A: RELEVANT LEGISLATION

11.1 Data Protection Act 1998

The Data Protection Act 1998 seeks to strike a balance between the rights of individuals and the sometimes competing rights of those with legitimate reasons for using personal information. It places obligations on those who process information (Data Controllers) while giving rights to those who are the subject of that data (Data Subjects). Anyone processing personal information must notify the Information Commissioner's Office that they are doing to, unless their processing is exempt.

The original Data Protection Act (1984) grew out of public concern regarding personal privacy in the face of rapidly developing computer technology and related to information held on computer systems. The Data Protection Act (1998) was passed in order to implement the European Data Protection Directive (95/46/EC). This Directive set a standard for Data Protection throughout all the countries in the European Union and applied to personal data held in a structured way in any medium (paper, computer, microfiche, tape etc). The new DPA extends the rights of individuals and increases the responsibilities of Data Controllers.

Personal data covers both facts and opinions about an individual. It also includes information regarding the intentions of the Data Controller towards the individual, although in some limited circumstances exemptions will apply. With processing, the definition is far wider than before. For example, it incorporates the concepts of 'obtaining', holding' and 'disclosing'.

The purpose of the Data Protection Act (1998) is to protect the rights and privacy of living individuals, to ensure that personal data are not processed without their knowledge and, in most cases, their consent. Any data held should be up-to-date, accurate, and securely stored. The Act includes information mechanically processed, manual filing systems and CCTV.

Personal data must be obtained fairly and lawfully. The data subject should be informed of who the Data Controller is and the purpose or purposes for which the data are intended to be processed; and to whom the data will be disclosed.

Personal data processing may only take place if specific conditions have been met. These include the data subject having given consent or the processing being necessary for the legitimate interests of the Data Controller.

Personal data must be kept accurate and up to date and shall not be kept for longer than is necessary.

Appropriate security measures must be taken against unlawful or unauthorised processing of personal data and against accidental loss of, or damage to, personal data. These include both technical measures, e.g. data encryption and the regular backing-up of data files and organisational measures, e.g. staff data protection training.

Any personal information given for one purpose must not be used for another purpose without the consent of the individual concerned the use may breach confidentiality.

The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than is necessary
6. Processed in line with your rights
7. Secure
8. Not transferred to other countries without adequate protection

The second area covered by the Act provides individuals with important rights, including the right to find out what personal information is held on computer and some paper records.

11.1.1 Definition of sensitive personal data

In this Act “sensitive personal data” means personal data consisting of information as to:

- (a) the racial or ethnic origin of the data subject,
- (b) his political opinions,
- (c) his religious beliefs or other beliefs of a similar nature,
- (d) whether he is a member of a trade union (within the meaning of the (1992 c. 52.) Trade Union and Labour Relations (Consolidation) Act 1992),
- (e) his physical or mental health or condition,
- (f) his sexual life,
- (g) the commission or alleged commission by him of any offence, or
- (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

11.1.2 Schedule 2 : processing of personal data

This schedule lists the conditions relevant for purposes of the first principle: **processing of any personal data**

- 1 The data subject has given his consent to the processing.
- 2 The processing is necessary—
 - (a) for the performance of a contract to which the data subject is a party, or
 - (b) for the taking of steps at the request of the data subject with a view to entering into a contract.
- 3 The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
- 4 The processing is necessary in order to protect the vital interests of the data subject.
- 5 The processing is necessary—
 - (a) for the administration of justice,
 - (b) for the exercise of any functions conferred on any person by or under any enactment,
 - (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
 - (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.
- 6 (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

11.1.3 Schedule 3: processing of sensitive personal data

This schedule lists the conditions relevant for purposes of the first principle: **processing of sensitive personal data**

- 1 The data subject has given his explicit consent to the processing of the personal data.
- 2 (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order—

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3 The processing is necessary—

(a) in order to protect the vital interests of the data subject or another person, in a case where—

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4 The processing—

(a) is carried out in the course of its legitimate activities by any body or association which—

(i) is not established or conducted for profit, and

(ii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5 The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6 The processing—

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7 (1) The processing is necessary—

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order—

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8 (1) The processing is necessary for medical purposes and is undertaken by—

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9 (1) The processing—

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of

equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10 The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

11.2 Freedom of Information Act 2000

The Freedom of Information Act (2000) was passed on 30 November 2000. This Act gives a general right of access to all types of 'recorded' information held by public authorities and sets out exemptions from that right. It places a number of obligations on public authorities, this also covers private organisations which provide public functions.

Anyone is able make a request for information, although the request must be made in writing, this includes email. The request must contain details of the applicant and the information sought. The Act gives applicants two related rights:

1. To be told whether the information is held by the public authority.
2. To receive the information (and where possible, in the manner requested, i.e. as a copy or summary, or the applicant may ask to inspect a record).

The Act is enforced by the Information Commissioner's Office (ICO); this role now combines Freedom of Information and Data Protection. Both the Freedom of Information Act and the Data Protection Act relate to information handling and the dual role will allow the ICO to provide an integrated and coherent approach.

The main features of the Freedom of Information Act are:

- A general right of access to information held by public authorities in the course of carrying out their public functions, subject to certain conditions and exemptions;
- In most cases where information is exempted from disclosure there is a duty on public authorities to disclose where, in the view of the public authority, the public interest in disclosure outweighs the public interest in maintaining the exemption in question;
- The Information Commissioner will implement the Act with wide powers to enforce the rights created;
- A duty imposed on public authorities to adopt a scheme for the publication of information. The schemes, which must be approved by the ICO, specifies the classes of information the authority intends to publish, the manner of publication and whether the information is available to the public free of charge or on payment of a fee.

The Act is retrospective in nature. It allows anyone, no matter who or where they are, to find out whether information is held, and if it is, to have access to it. It specifies exemptions covering information that does not have to be released (e.g. for personal information). It allows arrangements for enforcement and appeal and can result in imprisonment for contempt of court. Public authorities are obliged to provide information recorded both before and after the Act was passed.

Personal identifiable information is still governed by the Data Protection Act.

11.3 Data Protection and Freedom of Information – how do the two interact?

The Data Protection Act (1998) provides living individuals with a right of access to personal information held about them. The right applies to all information held in computerised form and also to non-computerised information held in filing systems structured so that specific information about particular individuals can be retrieved readily. Individuals already have the right to access information about themselves (personal data), which is held on computer and in some paper files under the Data Protection Act (1998). The right also applies to those archives that meet these criteria. However, the right is subject to exemptions, which will affect whether information is provided.

The Freedom of Information Act does not give individuals access to their personal information, though if a request is made, the Data Protection Act gives the individual this right. If the individual decides to make this information public it could be used alongside non-personal information gained by the public under the terms of the Freedom of Information Act. Other people cannot request access to personal information regarding other people.

11.4 The Information Commissioner

The Information Commissioner enforces and oversees the Data Protection Act (1998) and the Freedom of Information Act (2000). The Commissioner is a UK independent supervisory authority reporting directly to the UK Parliament and has an international role as well as a national one. In the UK, the Commissioner has a range of duties including the promotion of good information handling and the encouragement of codes of practice for data controllers, that is, anyone who decides how and why personal data, (information about identifiable, living individuals) are processed. For further information see The Information Commissioner website: www.ico.gov.uk

Contact: Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF; Fax: 01625 524 510; Enquiry/Information Line Tel: 01625 545 745;

E-mail: <http://www.esd.informationcommissioner.gov.uk/esd/genenq.asp>

11.5 Computer Misuse Act (1990)

The Computer Misuse Act became law in August 1990. Under the Act hacking and the introduction of viruses are criminal offences. All organisations both public and private need to co-operate to take action under the Act as the offences are likely to be committed by any employee of any status. For offences committed within many sectors the use of internal disciplinary measures are used rather than using legislation, however more employers are choosing to take criminal action.

The Computer Misuse Act (1990) identifies three specific offences

1. Unauthorised access to computer material (that is, a program or data). This would include: using another person's identifier (ID) and password without proper authority in order to use data or a program, or to alter, delete, copy or move a program or data, or simply to output a program or data.
2. Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime. This would include: gaining access to financial or administrative records, but intent would have to be proved.
3. Unauthorised modification of computer material. This would include: destroying another user's files; modifying system files; creation of a virus; introduction of a local virus; introduction of a networked virus; changing examination results; and deliberately generating information to cause a complete system malfunction.

The Act defines (1) (the basic offence) as a summary offence punishable on conviction with a maximum prison sentence of six months or a fine or both. The Act goes on to describe offences (2) and (3) as triable either summarily or on indictment, and punishable with imprisonment for a term not exceeding five years, a fine or both. These sentences clearly reflect the perceived gravity of the offence and would imply that any organisation should take an equally serious view of hacking or virus proliferation.

All organisations are primarily concerned with preserving the integrity of shared corporate computer systems. In the event of any problem information systems managers would expect to take immediate remedial and preventive action and would expect the organisation to support them up in this action with penalties in place which would serve to discourage hacking, particularly the third category which could result in a work being destroyed or in a complete system failure.

12. APPENDIX B – GLOSSARY OF TERMS

Aggregated

Data from a group of respondents or responding establishments which is combined at the data analysis stage so that information about the group as a whole is shown without identifying any individual respondent.

Anonymous data

Anonymous data are where the Data Controller does not have the means to identify an individual from the data they hold. If the Data Controller has information which allows the Data Subject to be identified, whether or not they intend to identify the individual is immaterial in the eyes of the Information Commissioner: this is not anonymous data. The Data Controller must be able to justify why and how the data are no longer personal.

Consent

The Information Commissioner's legal guidance to the Data Protection Act 1998 is to refer to the Directive, which defines consent as "...any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (3.1.5).

Data

- a) Information being processed by means of equipment operating automatically or
- b) Information recorded with the intention it be processed by such equipment.
- c) Recorded as part of a relevant filing system or
- d) Not in a or b or c, but forming part of an accessible record.

Data Controller

A person or a legal body, such as a business or public authority, who jointly or alone determines the purposes for which personal data are processed.

Data Controllers in common

When Data Controllers share a pool of personal data, each processing independently of the other.

Data Sharing Protocol

A local information sharing agreement outlining what information is going to be shared and for what purposes.

Data Flows

The movement of information internally and externally, both within and between organisations.

Data Processing

Any operation performed on data. The main examples are collection, retention, deletion, use and disclose.

Data Processor

Operates on behalf of the Data Controller. The Data Processor works with the data as defined by the data controller. The processor has no legal obligation regarding the data, any responsibility should be defined within the contract. Not staff.

Data Set

A defined group of information

Data Subject

An individual who is the subject of personal information.

Disclosure

The passing of information from the Data Controller to another organisation / individual

Establishment

The NMDS-SC definition of an establishment is: *“The operation at this single location, even if it comprises more than one building.”*

CSCI's working definition³ of an establishment is *“A place, including a building, in which organised activities are conducted”*.

Note that both definitions imply that an organised or managed operation or activity/ies is one of the key aspects of an establishment. Therefore, individually-managed local authority social work 'teams' can be treated for the purpose of completing the NMDS-SC as separate establishments, even if they operate from the same office or building.

Fair processing

To inform the Data Subject how the data are to be processed before processing occurs

Organisation

A business/legal entity

Personal Data

Data relating to a living individual who can be identified from those data (including opinion and expression of intention).

Purpose

The use and reason for which information is stored or processed.

Recipient

Anyone who receives personal information except statutory bodies for the purpose of specific inquiries

Sensitive Personal Data

Data regarding; racial origin, politics, trade union activity, health, sexuality, disability etc.

Subject Access

The individual's right to obtain a copy of information held about themselves.

Team

See 'Establishment' above.

Third Party

Any person who is not the data subject, the data controller, the data processor. Includes public sector bodies such as Department of Health, and members of the public).

³ The term establishment is not defined in the Care Standards Act. Within the case of Moore v Care Standards Tribunal and CSCI, (also known as 'Alternative Futures') a working definition was adopted of an establishment as "a place, including a building, in which organised activities are conducted" (source: CSCI guidance on sheltered accommodation)

13. APPENDIX C – NMDS-SC DATA ITEMS

Organisational data

The organisational information that is collected and stored on the system is:

- Establishment Name
- Parent Organisation Name (If Applicable)
- Address of Establishment
- Telephone Number
- E-Mail Address
- Registration with CSCI, Plus Number and date registered
- Investors In People Status
- Name of person completing questionnaire
- Job title of person completing questionnaire
- E-mail address of person completing questionnaire
- Date of completion
- Legal Status Of The Business (Private/Statutory Body)
- Services Provided
- Main Care Service Provided
- Type Of People Care Service Provided For
- Total Service Capacity
- Number Of Services Users At Time Of Completion
- Total Number of staff
- Number Of Staff Employed By Role
- Temporary/Permanent Employment
- Employment Started Within The Past 12 Months
- Temporary Staff Broken Down – pool, agency, student, voluntary, others
- Number Of Worker Ceased Employment In Past 12 Months
- Number Of Vacancies
- Reason For Leaving
- Where They Are Moving Onto

Worker data

The information about each worker that is collected and stored on the system is:

- National Insurance Number
- Home Postcode
- Gender
- Date Of Birth
- Ethnic Group
- Disability Status
- Date Of Completion
- Who Completed Questionnaire

- Main Job Role
- Other Job Roles
- Date Employment Commenced – main job
- Source Of Recruitment – main job
- Employment Status
- Contracted Hours
- Full Or Part Time Status
- Additional hours Worked within preceding 7 days
- Agreed Working Arrangements
- Sickness Level within preceding 12 months
- Salary
- Year Social Care Employment Began
- Continuity Of Employment
- Induction Training Undertaken
- Qualifications Held and year obtained
- Qualifications Currently Studying

14. APPENDIX D: NMDS-SC ONLINE SYSTEM CONTRACTUAL PROVISIONS

This appendix will contain a compilation of the clauses in the existing Contract between Skills for Care and its trusted supplier Tribal Ltd. Relevant to this Fair Processing Notice, and will follow.