Data Protection Policy

1. Scope

1.1 NCT Ltd (NCT) needs to collect certain types of personal information about the people with whom it deals, such as current, past and prospective students, employees, and those with whom it communicates. This information has to be collected for administrative purposes (such as staff recruitment and the administration of programmes of study), and to fulfill legal obligations to funding bodies and the government. The Data Protection Act 1998 requires that this information should be processed fairly, stored safely and not disclosed to any other person unlawfully. NCT is committed to protecting the rights and privacy of individuals in accordance with the requirements of the Data Protection Act. This document outlines NCT's policies in relation to the Data Protection Act.

1.2 NCT's Data Protection Policy applies to all students and staff of NCT. Any breach of the policy may result in NCT, as the registered data controller being liable in law for the consequences of the breach. Legal liability may also extend to the individual processing the data and his/her line manager under certain circumstances. In addition, breach of NCT's Data Protection Policy by staff or students will be considered to be a disciplinary offence and will be dealt with according to NCT's disciplinary procedures. Any member of staff or student who considers that the policy has not been followed with respect to personal data about themselves should raise the matter with their course coordinator or their line manager or the operations director.

1.3 This policy applies to all personal data for which NCT is responsible, including electronic data and manual data which are covered by the Data Protection Act. It applies regardless of where the data are held, and regardless of the ownership of the equipment used for processing, if the processing is performed for NCT purposes. Outside agencies and

NCT **Ltd, Baltic House, Tyne Dock, South Shields, Tyne and Wear, NE34 0AB**
Tel: **0845 058 3788** Fax: **0845 058 3789** Email: **info@nct-ltd.co.uk**

individuals who work with NCT, and who have access to personal information for which NCT is responsible, will be expected to comply with this policy and with the Data Protection Act.

2. Status of the Policy

This policy statement was approved by NCT's directors on 1st June 2008.

3. Definitions

This section explains terms which are commonly used in the Data Protection Policy.

3.1 Data controller

A person or organisation who makes decisions in regard to personal data, including decisions regarding the purposes for which and the manner in which personal data may be processed.

3.2 Data processor

An individual or organisation other than an employee of the data controller, who processes personal data on behalf of the data controller: e.g. a firm which collects and processes data on NCT's behalf under contract. Data controllers are responsible for the processing which is carried out for them by data processors, and have to ensure that this processing takes place within appropriate security arrangements.

3.3 Data subject

A living individual who is the subject of personal data.

3.4 Direct marketing

The communication of advertising or marketing material directed to particular individuals.

3.5 Manual data

Personal data which are not being processed by equipment operating automatically, or recorded with the intention that they should be processed by such equipment: e.g. data held in paper form.

3.6 Personal data

Data relating to a living individual who can be identified from the data, or from the data and other information which is in the possession of (or likely to come into the posession of) the data controller. Personal data include information such as an individual's name, home and work addresses, educational background, images and photographs (including CCTV footage), expressions of opinion about the individual, and the intentions of the data controller in regard to the individual.

3.7 Processing

Any operation on personal data, including obtaining, recording, holding, organising, adapting, combining, altering, retrieving, consulting, disclosing, disseminating, deleting, destroying and otherwise using the data.

3.8 Relevant filing system

A filing system for paper or other manual data which has been constructed in such a way that specific categories of information relating to an individual are readily accessible.

3.9 Sensitive personal data

Personal data relating to racial or ethnic origins, political opinions, religious beliefs, trade union membership, physical or mental health (including disabilities), sexual life, the commission or alleged commission of offences, and criminal proceedings.

3.10 Third parties

An individual or organisation other than the data subject, the data controller or a data processor acting on behalf of the data controller.

3.11 Vital interests

Although not defined in the Data Protection Act, the Information Commissioner has advised that "vital interests" should be interpreted as relating to life and death situations: e.g. the disclosure of a data subject's medical details to a hospital casualty department after a serious accident.

4. Data Protection Act Overview

4.1 The Data Protection Act 1998 commenced on 1 March 2000, with most of its provisions being effective from 24 October 2001. It replaced and broadened the Data Protection Act

1984. The purpose of the Act is to protect the rights and privacy of individuals, and to ensure that data about them are not processed without their knowledge and are processed with their consent wherever possible. The Act covers personal data relating to living individuals, and defines a category of sensitive personal data which are subject to more stringent conditions on their processing than other personal data.

4.2 The Data Protection Act covers data held in electronic formats, and also applies to manual data which are held in what the Act calls a relevant filing system. While this might appear to limit the categories of non-electronic data to which the Act applies, the definitions of personal data in the Data Protection Act have been broadened by the Freedom of Information Act 2000 in respect of public authorities to which the Freedom of Information Act applies. The main effect of this is that since 1 January 2005 (when the Freedom of Information Act came into force), unstructured personal information held by NCT in manual form - i.e. not in a relevant filing system - is covered by the Data Protection Act, except for unstructured data relating to appointments, removals, pay, discipline and other personnel matters, which remain outside the scope of the Act.

4.3 It should therefore be assumed, as a general rule, that any personal data relating to an identifiable living individual which are held by NCT in any form are covered by the Data Protection Act. However, unstructured manual data are exempt from many aspects of the Act, including the first, second, third, fifth, seventh and eighth Data Protection Principles, and from the sixth Data Protection Principle except in regard to the rights of data subjects to have access to their data and to require the rectification, blocking, erasure or destruction of inaccurate data.

4.4 NCT is a data controller in respect of the data for which it is responsible. This means that NCT is responsible under the Data Protection Act for decisions in regard to the processing of personal data, including the decisions and actions of external data processors acting on NCT's behalf. The Data Protection Act requires that processing should be carried out according to eight Data Protection Principles. These are outlined below, together with NCT's commitments to upholding these principles:

4.5 Data Protection Principles

4.5.1 (Principle 1) Personal data shall be processed fairly and lawfully.

NCT will ensure that data are obtained fairly, and will make reasonable efforts to ensure that data subjects are told who the data controller is, what the data will be used for, for how long the data will be kept and any third parties to whom the data will be disclosed. In order for processing to be fair and lawful, data which is not sensitive personal data will only be processed by NCT if at least one of the following conditions, set down in the Data Protection Act, has been met:

1. The data subject has given his/her consent to the processing.
2. The processing is necessary for the performance of a contract with the data subject, or for taking steps with a view towards entering into a contract.
3. The processing is required under a legal obligation other than a contract.
4. The processing is necessary to protect the vital interests of the data subject.
5. The processing is necessary for the administration of justice, the exercise of functions under an enactment, the exercise of functions of the Crown or a government department, or any other functions of a public nature exercised in the public interest.
6. The processing is necessary to pursue the legitimate interests of NCT or of third parties, and does not prejudice the rights, freedoms or legitimate interests of the data subject.

4.5.2 Processing of sensitive personal data is subject to more stringent restrictions under the Data Protection Act. Processing of sensitive personal data will only be carried out by NCT if at least one of the above conditions, applicable to non-sensitive data, has been met. In addition, at least one of the following conditions, set down in the Data Protection legislation, must also be met:

1. The data subject has given his/her explicit consent.
2. The processing is required by law in connection with employment.
3. The processing is necessary to protect the vital interests of the data subject or another person.
4. The information has been made public by the data subject.
5. The processing is necessary for legal proceedings, obtaining legal advice, or establishing or defending legal rights.
6. The processing is required for the administration of justice, the exercise of functions under an enactment, or the exercise of functions of the Crown or a government department.
7. The processing is necessary for medical purposes, and is carried out by a health professional or a person with an equivalent duty of confidentiality.
8. The processing is necessary to trace equality of opportunity between people of different racial or ethnic backgrounds, different religious beliefs, or different states of physical or mental health or physical or mental conditions.
9. The processing is in the substantial public interest, and is necessary for preventing or detecting any unlawful act or failure to act.
10. The processing is in the substantial public interest, and is necessary for the protection of the public against dishonesty, malpractice, unfitness, incompetence, seriously improper conduct, mismanagement in the administration of services or failure in services.
11. The processing is in the substantial public interest, and involves the publication of information relating to point (10) or publication for the purposes of journalism, literature or art.
12. The processing is in the substantial public interest, and is necessary for the functions of a counseling service.
13. The processing is in the substantial public interest, and is necessary for research purposes; provided that the processing will not support measures or decisions with regard to individuals, and will not cause substantial damage or distress to the data subject or any other person.

This list omits some conditions relating to the processing of sensitive personal data which are unlikely to be relevant to NCT.

4.5.3 Data relating to the disabilities of students, staff and other individuals are sensitive personal data under the Data Protection Act. Such data must be processed in accordance with NCT's Disability Policy.

4.5.4 (Principle 2) Personal data shall be obtained only for a specified and lawful purpose or purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.

NCT will ensure that data which are obtained for a specified purpose are not used for a different purpose, unless that use is done with the consent of the data subject, is covered by NCT's registration with the Information Commissioner, or is otherwise permitted under the Data Protection Act.

4.5.5 (Principle 3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

NCT will not collect personal data which are not strictly necessary for the purpose or purposes for which they were obtained.

4.5.6 (Principle 4) Personal data shall be accurate and, where necessary, kept up to date.

NCT will take reasonable steps to ensure the accuracy of personal data which it holds, and will take steps to correct inaccurate data when requested to do so by a data subject.

4.5.7 (Principle 5) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

NCT will ensure that personal data are not kept for longer than is required by the purpose or purposes for which the data were gathered. NCT may retain certain data indefinitely for research purposes (including historical or statistical purposes), as permitted under the Data Protection Act, subject to the conditions laid down in the Act for this type of processing.

4.5.8 (Principle 6) Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.

NCT will ensure that personal data are processed in accordance with the rights of data subjects under the Data Protection Act. These rights include the right to:

- Make subject access requests to find out what information is held about them, the purposes for which it will be used, and to whom it has been disclosed.
- Prevent the processing of data which is likely to cause them substantial damage or substantial distress.
- Prevent processing for the purposes of direct marketing.
- Be informed about automated decision making processes that affect them.
- Prevent significant decisions that affect them from being made solely by automated processes.
- Sue for compensation if they suffer damage through contravention of the Act.
- Take action to require the rectification, blocking, erasure or destruction of inaccurate data.
- Request an assessment by the Information Commissioner of the legality of any processing that is occurring.

4.5.9 (Principle 7) Appropriate technical and organisational measures shall be taken to prevent the unauthorised or unlawful processing of personal data and the accidental loss, destruction of or damage to personal data.

NCT will take steps to ensure the security of personal data which are held electronically and in manual form, to prevent the unauthorised disclosure of data to third parties, and loss or damage to data that may affect the interests of data subjects. NCT will also ensure that data processors provide an appropriate level of security for the personal data which they are processing on NCT's behalf.

4.5.10 (Principle 8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

NCT will not transfer data outside the European Economic Area unless the transfer would be permitted under the Data Protection Act

4.5.11 The Data Protection Act requires bodies which record and use personal information to register with the Information Commissioner. NCT's registration details are included in the Register of Data Controllers which is available on the website of the Information Commissioner. It records the purposes for which NCT gathers personal data, the types of data subjects covered by each purpose, the classes of data gathered, recipients to whom the data will be disclosed, and countries or territories to which the data may be transferred. Any use by NCT of personal data must be in accordance with the terms of NCT's registration.

4.5.12 Information about how NCT processes data relating to its students is contained in the Student Data Protection Statement. This explains to students what data NCT collects about them; how their information will be used by NCT while they are a student and after they

cease to be a student; what external agencies may receive their data; and what their rights and responsibilities are in regard to their data. The statement expands on the more general information about the processing of personal data which is contained in this Policy.

4.5.13 Further information about the Data Protection Act is available on the website of the Information Commissioner.

5. Staff Responsibilities

5.1 NCT as a corporate body is a data controller under the Data Protection Act. NCT's directors have oversight of planning and policy development matters in the area of information compliance, including Data Protection. The Administration Team Leader deals with day to day Data Protection matters, such as subject access requests. The Managing Director is a point of contact for issues relating to Data Protection.

5.2 When processing personal data, NCT staff must ensure that they abide by the Data Protection Act, this policy and any related policies and procedures. NCT must only process personal data in accordance with its registration with the Information Commissioner. The registration defines, in a very general way, the purposes for which NCT processes personal data and related information, and is available on the Information Commissioner's website as part of the Register of Data Controllers. In practice, most routine uses of personal data will be covered by NCT's registration and will be legitimate from a Data Protection standpoint. However, this will not necessarily be the case where changes are introduced to the way in which data are processed - such as using the data for a purpose for which the data have not previously been used, or transferring the data to a new source.

5.3 Before such changes are introduced, staff should check to ensure that the proposed changes will be in accordance with NCT's registration with the Information Commissioner, and will comply with the Data Protection Act and this Policy. Staff who are uncertain as to whether their processing of data meets these requirements should refer any queries to their line manager in the first instance. Staff should also ensure that any personal information for which they are responsible is accurate and up to date, including information which NCT holds about themselves (e.g. their home address), and that data for which they are responsible are kept secure and are not disclosed to unauthorised parties.

5.4 Data should only be transferred internally within NCT when there is a genuine business need to do so. Staff who receive transferred data are equally responsible for ensuring that the data are processed in accordance with this policy and NCT's obligations under the Data Protection Act. It is important that internally transferred data should continue to be used for purposes which are consistent with the purposes which applied when the data was gathered, to avoid violation of the second Data Protection Principle. Particular care should be taken when disclosing personal data to parties outside the NCT.

5.5 Team leaders/managers of administrative departments are responsible for ensuring that the processing of personal data in their department conforms to the requirements of the Data Protection Act and this policy. In particular, they should ensure that new and existing staff who are likely to process personal data are aware of their responsibilities under the Act. This includes drawing the attention of staff to the requirements of this policy, and ensuring that staff who have responsibility for handling personal data are provided with adequate training.

5.6 Team leaders/managers must also see that correct information and records management procedures are followed in their departments (see Records Management procedure). This includes establishing retention periods to ensure that personal data are not kept for longer than is required.

5.7 Staff should also note that NCT is not responsible for any processing of personal data by them which is not related to their employment with NCT, even if the processing is carried out using NCT's equipment and facilities. Staff are personally responsible for complying with the Data Protection Act in regard to data for which they are the data controller.

6. Gathering Data

6.1 Any gathering of personal data by members of NCT must be accordance with NCT's registration with the Information Commissioner. Staff should consult with the Administration Team Leader or Managing Director before introducing any new form of data gathering or making changes to existing methods of data gathering. If it appears that the collection of the data would not be covered by NCT's existing registration, the Managing Director must be informed before the changes are implemented, so that NCT's register entry can be updated.

6.2 While it is not always necessary to have the consent of the data subject in order for the processing of data to be fair and lawful, it is advisable to seek consent wherever possible, particularly in regard to sensitive personal data where explicit consent should normally be obtained. NCT also has a general obligation under the first Data Protection Principle to ensure that data subjects are provided with information about how their data will be used by NCT, unless doing so would involve disproportionate effort. To meet these requirements, paper and electronic forms (including web based forms) created by NCT which gather personal data should always include a fair processing notice.

It is recommended that fair processing notices used on NCT forms should explain:

- Why the data needs to be gathered and how the data will be used **[essential]**.
- The parts of NCT that will use the data **[desirable]**.
- Any third parties outside NCT to whom the data will be disclosed or transferred **[essential]**.

- How long the data will be kept **[desirable]**.
- The fact that completion of the form will be taken as consent by the data subject to the use of the data as outlined **[essential]**.
- How the data subject can exercise his/her rights under the Data Protection Act (e.g. by linking to NCT's Data Protection web pages or by providing contact details for NCT's Information Compliance Manager) **[desirable]**.

6.3 To avoid infringement of the third Data Protection Principle, forms and other methods of data collection should not gather more data than are necessary for the task at hand. Staff who are responsible for the design of forms should ensure that there is a clear business need for each data item requested. Otherwise, the form should be amended to remove the data item.

6.4 Data subjects have the right to prevent the processing of their data for direct marketing purposes (e.g. promotional mailshots). If personal data gathered via a form is to be used for direct marketing, the form must also include:

- A statement explaining how the data will be used for direct marketing.
- Information on how the data subject can opt out of the use of the data for that purpose (e.g. by ticking a box).

6.5 Where direct marketing is involved, the form should indicate that it is assumed that the data subject consents to the use of the data for direct marketing purposes unless he/she specifies otherwise.

6.6 Information about visitors to a website gathered through cookies, web bugs and other devices will become personal data if the data is linked to personal details of the user, such as name and address details submitted through an online form. NCT websites which use cookies, web bugs and other tracking devices in this way should include a privacy statement explaining:

- Which data will be collected in this way.
- Which parts of NCT will use the data.
- How the data will be used.
- How long the data will be kept.
- How users can disable cookies, web bugs and other devices if they wish to do so.

7. Disclosure of Data

7.1 Staff must take particular care when disclosing personal data to third parties to ensure that there is no breach of the Data Protection Act or the law of confidence.

7.2 Disclosure may be unlawful even if the third party is a family member of the data subject, or a local authority, government department or the police. A key point to consider is whether the disclosure is relevant to and necessary for the conduct of the organisation's business. For example, it would generally be appropriate to disclose a staff member's work contact details in response to an enquiry relating to a function for which they are responsible, but it would not be reasonable or appropriate to disclose a staff member's personal address or bank account details.

7.3 The disclosure of personal data represents a form of processing of the data. This means that the conditions for fair and lawful processing of personal data and sensitive personal set out in first Data Protection Principle must be met. Consideration should also be given as to whether the disclosure was one of the purposes for which the data were originally gathered; in particular, whether the disclosure is covered by NCT's entry in the Information Commissioner's Register of Data Controllers, or is a purpose to which the data subject has consented. If not, the disclosure is likely to represent further processing contrary to the second Data Protection Principle.

7.4 Disclosure of personal data which are not sensitive personal data is most likely to be justified if one or more of the following conditions applies:

- The data subject has given his/her consent to the disclosure (e.g. at the time when the data were gathered).
- The disclosure is in the legitimate interests of NCT or of the third party to whom the data are to be disclosed, and does not prejudice the rights, freedoms or legitimate interests of the data subject.
- There is a statutory or legal obligation to disclose the data.
- The disclosure is required for the performance of a contract (e.g. between a student and a sponsor).
- The disclosure is necessary to protect the vital interests of the data subject.

7.5 More stringent restrictions apply to the processing of sensitive personal data. The most likely conditions that would justify disclosure of sensitive personal data are:

- The data subject has given his/her explicit (ideally written) consent to the disclosure, or
- There is a statutory or legal obligation to disclose the data, or
- The disclosure is necessary to protect the vital interests of the data subject.

7.6 The Data Protection Act also allows personal data to be disclosed to third parties without the consent of the data subject, in the following circumstances:

- The disclosure is necessary for safeguarding national security.
- The disclosure is necessary for the prevention or detection of crime, or the apprehension or prosecution of offenders.

- The disclosure is necessary for the assessment or collection of any tax or duty.
- The disclosure is necessary for the discharge of regulatory functions (including the health, safety and welfare of people at work).
- The data to be disclosed are to be used for research purposes, subject to the rules governing the use of data in research.
- The data are information which NCT is obliged by legislation to provide to the public.
- The disclosure of the data is required by legislation, rule of law or the order of a court. For example, certain data on students and staff have to be supplied by NCT to the Learning and Skills Council and Tyne and Wear Care Alliance (where they are the funding body).

7.7 The Freedom of Information Act 2000 sets out certain circumstances in which personal data can be disclosed to a third party (i.e. someone other than the data subject) who has submitted a Freedom of Information (FoI) request. In particular, the FoI Act provides that personal data can be disclosed where doing so would not breach any of the Data Protection Principles. Guidance from the Information Commissioner suggests that this is likely to apply to data relating to an individual's official or work capacity which it would normally be reasonable to release, such as name, job title, official functions, grade, decisions made in an official capacity, and salaries of senior staff. Data relating to an individual's private life would not normally be disclosable under FoI.

7.8 There are also two other special situations where the FoI Act allows personal data to be released to a third party in response to an FoI request, provided a public interest test has been met:

- The data controller has received a formal objection from the data subject, under the Data Protection Act, to the disclosure of the data (known as a Section 10 Notice).
- The release of the data to the data subject would be prevented by one of the exemptions in the Data Protection Act.

7.9 In such cases, there is no automatic requirement to release the data to the third party, but data controllers have to consider whether it would be in the public interest to release the data. Such cases are likely to be rare.

7.10 FoI requests for the release of personal data to third parties need to be handled according to the rules set down in the FoI Act, which are different from those in the Data Protection Act (for further information, see “Submitting a Freedom of Information Request”. Any release of personal data in response to an FoI request should be cleared in advance with the organisation’s Administration Team Leader. In addition, it should be noted that the FoI Act does not grant individuals any right to request data relating to themselves.

7.11 Staff should always exercise caution when dealing with requests from third parties for the disclosure of personal data. Disclosure requests should normally be required to be in writing, and should be responded to in writing. Where reasonable, the party making the

request should be required to provide a statement explaining the purpose for which the data is requested, the length of time for which the data will be held, and an undertaking that the data will be held and processed according to the Data Protection Principles. Where the request relates to the prevention/detection of crime, the apprehension/prosecution of offenders, assessment/collection of any tax or duty, or the discharge of regulatory functions, appropriate paperwork should be produced by the enquirer to support their request (e.g. official documentation stating that the information is required in support of an ongoing investigation). Guidance for staff on how to respond to requests for data from the police and similar agencies is available in NCT's Police Disclosure Guidelines.

7.12 Personal data should only be disclosed over the telephone in emergencies, where the health or welfare of the data subject would be at stake. If data have to be disclosed by telephone, it is good practice to ask the enquirer for their number and to call them back. For further information on how to respond to emergency requests, see the Police Disclosure Guidelines.

7.13 Particular care should be taken when dealing with requests from embassies and high commissions, as data subjects may choose to have little or no contact with representatives of their home states. Similarly, members of NCT may have reasons for not wanting contact with parents, other relatives or friends. Requests from relatives, friends etc for the contact details of students should therefore be treated with caution. It is good practice to offer to pass on any message without providing contact details or confirming or denying that the person is a member of NCT.

7.14 An image of an identifiable individual is personal data about them. In some situations, publication of an image without the individual's permission will infringe their right to privacy and the Data Protection Act. Only images from approved websites will be used where it is know permission has been given. Permission will be obtained from staff and learners where images are used in marketing material and on the website. Where learners consent to take part in publicity and promotional activities, then it will be assumed that consent has been given.

8. Transfer of Information

8.1 NCT has a contractual obligation to transfer information to the Learning Skills Council (LSC) or the Tyne & Wear Care Alliance (TWCA) whichever is the students funding body. Some of the information may be sensitive personal data and appropriate precautions will be taken when processing information. The LSC is responsible for funding, planning and encouraging education and training for young people and adults in England, and is registered under the Data Protection Act 1998. The information provided will be shared with other organisations for the purpose of administration, careers and other

guidance, and statistical and research purposes. Other organisations with which they will share information include, the Department for Education and Skills, Connexions, Higher Education Statistics Agency, Higher Education Funding Council for England, educational institutions and organisations performing research and statistical work on behalf of the LSC or its partners. The LSC also administers the learner registration service (LRS) which will use information to create and maintain a unique learner number (ULN).

9.Transfer Outside the EEA

The eighth Data Protection Principle (see Data Protection Act Overview)) requires that personal data must not be transferred outside the European Economic Area (the European Union member states plus Iceland, Norway and Liechtenstein), unless the country or territory to which the data are to be transferred provides an adequate level of protection for personal data.

The European Commission has recognised a number of non-EEA countries which it deems to provide an adequate level of protection for personal data. Transfer of data to these countries will not violate the eighth Data Protection Principle. Similarly, the eighth Data Protection Principle will not be violated if transfer occurs in the following circumstances:

- The data is transferred to a company in the United States which has signed up to the 'Safe Harbour' agreement (a set of rules similar to those found in the UK's data protection law).
- The transfer is made under a contract which includes the model clauses adopted by the European Commission to ensure that there will be adequate safeguards for data transferred to a source outside the EEA.

Further information about the EC's list of approved countries, the 'Safe Harbour' agreement and the EC's model contractual clauses is available on the website of the Information Commissioner.

The Data Protection Act also contains a number of exemptions to the eighth Data Protection Principle. The transfer of personal data outside the EEA is permitted (regardless of the country to which the data are transferred or the receiving organisation), where at least one of the following applies:

- The data subject has given his/her consent to the transfer.
- The transfer is necessary for the performance of a contract between the data controller and the data subject; or a contract between the data controller and a third party which has been entered into at the request of the data subject, or is in the interests of the data subject.
- The transfer is necessary for legal proceedings or defending legal rights.
- The transfer is necessary for reasons of substantial public interest.
- The transfer is necessary to protect the vital interests of the data subject.

- The transfer is part of the personal data on a public register.

The European Court of Justice has determined that making personal data available on a website does not contravene the Data Protection rules prohibiting the transfer of data outside the EEA (ECJ Case C-101/01 Criminal proceedings against Bodil Lindqvist). However, while it may not contravene the eighth Data Protection Principle, placing personal data on the Internet must still be done in a way that complies with the other Data Protection Principles, such as the need to ensure that the processing is fair and lawful.

9.Publication of Data

9.1 NCT routinely publishes a number of items that include personal data, and will continue to do so. These include staff information (such as name, department, job title, email address and telephone number) in the NCT website, information in prospectuses, annual reports, newsletters, e-bulletins, guides, etc.

9.2 Any individual who has good reason for wishing their details in such publications to remain confidential should contact the Administration Team Leader.

10. Security of Data

10.1 The seventh Data Protection Principle (see Data Protection Act Overview)) requires that precautions should be taken against the physical loss or damage of personal data, and that access to and disclosure of personal data should be restricted. Members of NCT who are responsible for processing personal data must ensure that personal data are kept securely, and that personal information is not disclosed orally or in writing, by accident or otherwise, to unauthorised third parties.

10.2 Information security is a large area, so the following recommendations are meant as general guidance only. They apply equally to data processed off-site (e.g. by staff at home or on laptops), as to data processed on NCT premises. In fact, off-site processing presents a potentially greater risk of accidental loss, theft or damage to data.

Manual data

- When not in use, files containing personal data should be kept in locked stores or cabinets to which only authorised staff have access.
- Procedures for booking files in and out of storage should be developed, so that file movements can be tracked.
- Files should be put away in secure storage at the end of the working day, and should not be left on desks overnight.

Electronic data

Members of NCT using the company's IT systems must conform to the "Information Technology Policy". Attention is drawn in particular to the following policies, which are directly relevant to the security of personal data and other data for which NCT is responsible:

- Conditions of Use of IT systems (covering security of usernames, passwords, shared file areas etc).
- IT Security Policy (covering overall responsibility for IT security).
- Policy for Use of Information Servers (duties of staff responsible for servers).
- Equipment and Software used by Individuals and Workgroups (authorised use of hardware and software).

10.3 Care must be taken to ensure that PCs and terminals on which personal data are processed are not visible to unauthorised persons, especially in public places. Screens on which personal data are displayed should not be left unattended. Particular care must be taken when transmitting personal data. Appropriate security precautions, such as the use of encryption and digital signatures, should be taken when sending personal data by email. Transmission of personal data by fax should generally be avoided.

10.4 As well as preventing unauthorised access, it is equally important to avoid the accidental or premature destruction of personal data which could prejudice the interests of data subjects and of NCT. To prevent the accidental loss of electronic data, members of NCT should ensure that storage of personal data in electronic form conforms to the good practice guidelines set down in NCT's Code of Practice for Electronic Data Storage, Transmission and Backup.

10.5 Personal data in both manual and electronic formats should only be destroyed in accordance with agreed retention schedules. Care must be taken to ensure that appropriate security measures are in place for the disposal of personal data. Manual data should be shredded or disposed of as confidential waste, while hard drives, disks and other media containing personal data should be wiped clean (e.g. by reformatting, over-writing or degaussing) before disposal. Disposal of electronic media and equipment should be in accordance with NCT's Procedure for Disposing of Information Technology Equipment and Packaging.

10.6 The Data Protection Act lays particular obligations on data controllers to ensure that there are adequate safeguards for processing which is carried out on their behalf by data processors. Whenever personal data is to be processed by an external body acting on NCT's behalf, NCT must:

- Choose a data processor which provides sufficient guarantees in regard to its technical and organisational security measures;
- Take reasonable steps to ensure that the data processor complies with these measures, and
- Ensure that the processing takes place under a written contract which stipulates that the processor will act only on instructions from NCT, and that the processor will have security measures in place that ensure compliance with the seventh Data Protection Principle.

11. Use of Data in Research

11.1 The Data Protection Act 1998 sets down certain exemptions which allow personal data to be used for research purposes (including historical or statistical research), where the data were originally gathered fairly and lawfully for other purposes. Data collected for one purpose or piece of research can be used for other research, and can be kept indefinitely, provided the following conditions are met:

- The data must be used solely for research purposes, and not for any other purposes (e.g. general administration) unless those purposes are the same as the purposes for which the data were gathered.
- The data must not be processed to support measures or decisions in regard to particular data subjects.
- The processing for research purposes must not cause, or be likely to cause, substantial damage or distress to data subjects. Closure of the data to outside access would be one way of helping to ensure this, as would anonymisation of research results.

11.2 Where the above conditions have been met, data retained for research purposes are exempt from subject access requests, provided the results of the research are not published in a form which identifies the data subjects. However, other aspects of the Data Protection Principles will still apply, such as the requirement to keep the data secure, and the requirement that the data should be processed fairly and lawfully.

11.3 In addition to the exemptions in the Data Protection Act, the Data Protection (Processing of Sensitive Personal Data) Order 2000 allows sensitive personal data to be retained in archives for research purposes, provided:

- The processing for research purposes is in the substantial public interest;
- The data are not used to make decisions about individuals without their consent; and
- The processing for research purposes does not cause substantial damage or distress to any person.

12. Examinations and Assessment

12.1 Examination scripts - i.e. the information recorded by candidates in exams - are exempt from data subject access requests under the Data Protection Act 1998. NCT is under no

obligation to permit candidates to have access to completed scripts or copies of scripts. However, comments by internal and external examiners made on examination scripts or in a form which allows them to be related to original scripts are covered by the Data Protection Act, and may be the subject of access requests. Examination marks can also be requested. If an access request is made before the examination results are announced, the timescale for responding to requests is extended to five months from the date of the request, or 40 days from the announcement of the results (whichever is earlier).

12.2 Examinations are defined in the Data Protection Act as "any process for determining the knowledge, intelligence, skill or ability of a candidate by reference to his performance in any test, work or other activity". This means that other forms of assessment (e.g. written assessment work, field work) are covered by the same provisions as those relating to examinations.

For information on how to submit a Data Protection request to NCT, see Requesting Access to Personal Data.

13. References and Recruitment

13.1 Confidential references for educational or employment purposes will involve the disclosure of personal information, often of a private nature. Requests for references which are received from reputable organisations and which request that the reference is returned to a recognised address can generally be taken at face value, where it is known that the individual who is the subject of the request has cited a member of NCT as a referee. However, if there is any doubt as to the validity of a reference request, staff should always check with the individual concerned to determine that they are willing for information about them to be released. Staff who are requested to provide references in their work capacity must ensure that they do so in accordance with NCT's Staff References Policy.

13.2 References given by a data controller are exempt from data subject access requests under the Data Protection Act. In practical terms, this means that NCT is under no obligation to disclose the data contained in copies of references given by NCT staff. However, references received by a data controller are not exempt from subject access requests. This has the following implications, which should be taken into consideration by staff who are asked to provide references:

- References received by NCT from other individuals or organisations may have to be disclosed in response to subject access requests directed at NCT.
- References from NCT to other organisations may have to be disclosed by those organisations in response to subject access requests.

13.3 A reference will also contain personal data about the referee, such as the referee's name and address, and possibly confidential information about the referee or third parties. The information contained in a confidential reference need not be released if it would identify the referee, unless one of the following conditions can be satisfied:

- The referee's identity can be protected by anonymising the information.
- The referee has consented to the release of the data.
- It is reasonable in all circumstances to release the information without the referee's consent.

13.4 Guidance has been issued by the Information Commissioner on handling subject access requests for references, which emphasises that such requests should be dealt with on a case by case basis. All requests from data subjects for access to references should be referred to the Administration Team Leader.

13.5 Given the possibility that a reference may be disclosed as a result of a Data Protection Act request, referees should avoid making statements in references which cannot be supported by factual evidence. See NCT's Staff References Policy for further guidance.

13.6 Staff involved in recruitment and selection should be aware that information in documents such as interviewers' notes could potentially be disclosed to data subjects in response to access requests. Staff should therefore ensure that any feedback which is provided to candidates after interview is consistent with and can be supported by the documentation relating to the recruitment and selection process. Feedback should be provided in a manner which complies with NCT's Recruitment Policy and Procedure and Best Practice Guidelines on Feedback.

14. Retaining Data

14.1 The Data Protection Act 1998 does not specify periods for the retention of personal data. It is left to data controllers to decide how long personal data should be retained, taking into account the Data Protection Principles, business needs and any professional guidelines. In the context of NCT, the following factors need to be taken into consideration:

- The need to balance the requirement of the fifth Data Protection Principle - that personal data should not be kept for longer than necessary - against the need to prevent the premature or accidental destruction of data which would damage the interests of data subjects, contrary to the seventh Data Protection Principle.

- The exemptions provided by the Data Protection Act which allow the permanent retention of data for historical and statistical research. NCT's history should not be endangered by the overzealous destruction of data that could be retained as historical archives.
- The fact that the Data Protection Act does not override provisions in other legislation (e.g. health and safety legislation) which specify retention periods for personal data.

14.2 A retention schedule is a device used by records managers to specify retention periods for series of paper and electronic records. A retention schedule has been developed for NCT covering the major series of the company's records (i.e. focusing on those which NCT generates in large

quantities). Advice on retention periods relating to personal data is available from the Administration Team Leader.

14.3 Staff should note that under the Freedom of Information Act, it is a criminal offence to deliberately alter, deface, block, erase, destroy or conceal data which has been the subject of an access request under the Data Protection Act or the Freedom of Information Act with the intention of preventing the release of the data. However, data may be amended or deleted after receipt of the access request but before disclosure of the data, if the amendment or deletion would have taken place regardless of the request (e.g. under a retention schedule).

15. Records Management

15.1 Effective management of paper and electronic records is essential for compliance with the Data Protection Act and other legislation, such as the Freedom of Information Act. In the context of Data Protection, good records management ensures that personal data contained in records:

- Can be located in response to subject access requests and business needs.
- Are protected from accidental loss or destruction.
- Are retained according to established retention periods.
- Are secured against unauthorised access and disclosure.
- Are preserved for future use, where necessary, in formats suitable for long-term preservation.

15.2 Team leaders/managers of relevant administrative departments are responsible for ensuring the effective management of records in their sections. Staff who require advice or assistance on records management issues should contact the Administration Team Leader.

16. Access to Data

16.1 The purposes for which NCT processes personal data and the types of data processed for each purpose have been registered with the Information Commissioner. Details of NCT's registration are contained in the Information Commissioner's Register of Data Controllers.

16.2 The Data Protection Act gives data subjects the right of access to personal data which NCT holds about them. Anyone who wishes to exercise this right should apply in writing to

the Administration Team Leader. NCT charges a fee (currently £10.00) for each Data Protection request, and requires proof of identity to prevent the unlawful disclosure of personal data. For further information about how to submit a request (including the form to use) and how requests are processed, see “Requesting Access to Personal Data”.

16.3 NCT will respond to subject access requests as quickly as possible, and is required by law to respond within 40 days of receipt of the request, fee and proof of identity. In some cases, NCT may not release information because the data are subject to exemptions under the Data Protection Act, or doing so would release personal data relating to other individuals. See Requesting “Access to Personal Data” for further information about the circumstances in which NCT may not release data.

16.4 If the requested data are located and can be released, the data subject will normally be provided with the information in permanent form on paper: e.g. as a printout, photocopy, transcript or transcription.

16.5 The Freedom of Information Act does not give individuals any right of access to data relating to themselves. Where a Freedom of Information request requires access to data relating to the person making the request, he/she will be asked to re-submit the request to NCT as a Data Protection Act request. For further information on how to submit a Freedom of Information Act request and how NCT processes requests, see “Submitting a Freedom of Information or Environmental Information Request”.

16.6 Staff who receive a request which they believe to be a request for data under the Data Protection Act should pass the request on to the Administration Team Leader as soon as possible. It is advisable to pass on all requests where the individual seeks information about themselves, even if they do not mention the Data Protection Act, unless the request is for information which would normally be released as a matter of routine. Under no circumstances should staff deliberately alter, conceal or destroy data which has been the subject of an access request in order to prevent the release of the data.