TEN Group Data Protection Policy

Policy number:	DP01
Version:	1.0
Policy holder:	David Brown
Approval board:	TEN Group Board
Date of approval:	Feb 2014
Review period:	Annual
Date of latest review:	
Next review date:	Feb 2015
Legislation or regulation:	• The Data Protection Act • Privacy and Communications (EC Directive) Regulations 2003 • Computer Misuse Act 1990 • Freedom of Information Act 2000 • Protection of Freedoms Act 2012 • Regulation of Investigatory Powers Act (2000) • Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000

Version Control Document

Date	Version No.	Reason for Change	Author
July 2013	v0.1	Initial Draft	Diana Bowie
August 2013	V0.2	Amendments to Initial Draft	Diana Bowie
October 2013	V0.3	Amendments to Second Draft	Diana Bowie
January 2014	V0.4	Amendments to Final Draft	Diana Bowie
February 2014	V0.5	Amendments to Final Draft	Diana Bowie

Contents

1. Data Protection Policy Statement

Statement of Intent

Transforming Education in Norfolk (TEN) Group is committed to fostering high standards of data protection in all processing of personal data relating to the Federation's employees and pupils/students, contractors and visitors. In particular, the Group will work to ensure so far as is reasonably practical, that all legal obligations under the Data Protection Act 1998 (DPA) and successor legislation are met by the Federation Organisations.

The TEN Group Board & Group CEO actively promotes a culture whereby the 8 Principles of the DPA are known, understood and embedded into day to day processing, and that data protection/privacy considerations are acknowledged early in the planning of any new or changed activity so that exposure to risk is minimised and/or managed. The TEN Group Board & Group CEO will achieve this, so far as is reasonably practicable via Federation Organisations, who are the Data Controllers for the individual institutions, who are required to;

- ensure that personal data is processed fairly and lawfully, and only for the specified purposes identified with the Information Commissioner's Office (ICO)
- allocate a member of staff to maintain specific responsibility for data protection;
- ensure that privacy impact assessments are undertaken for new or changed processing involving personal data
- implement a data protection compliance system to include regular audits, inspections and a review of actions arising;
- ensure that appropriate Data Sharing Agreements are in place where regular sharing of personal data takes place
- Undertake effective preliminary checks and implement strong Data Processor Agreements where third party processors are engaged
- ensure consultation takes place with staff and pupils/parents or students on matters relating to data protection;
- provide adequate information instruction and training for staff and pupils/parents and students;
- provide adequate resources to guarantee secure processing of personal data undertaken at any of their managed sites or at any other workplace.

Specific responsibilities for data protection within the TEN Group are set within this policy under Data Protection, copies of which can be downloaded from the intranet or requested from the TEN Group.

The Data Protection Policy is intended to enable the Federation Organisations, their management and staff to work together in partnership, to meet their responsibilities in relation to their roles as Data Controllers and data processors. It will be reviewed annually by the TEN Group Board.

Ms B Falkus
Chairman of the TEN Group Board

Mr R Palmer
Group CEO

2. Definitions

2.1 What is Personal data?

Under the Data Protection Act (DPA) personal data is or may be

- About a living, identifiable individual
- Relating to such an individual
- Forming part of an accessible record
- Held or intended to be held electronically
- Held in a relevant filing system.

Personal data includes data which when brought together with other information held allows a living individual to be identified e.g. a name and date of birth, a list of names with associated course information, a name and image. Even anonymised information e.g. statistics can be deemed to disclose personal data where an individual's particular circumstances are unique.

2.2 Sensitive personal data

Some data is classed as 'sensitive' within the terms of the DPA. This type of data is subject to further regulation under the DPA and can only be processed under certain circumstances.

Personal data becomes 'sensitive' if it includes any of the following types of personal data about an identifiable, living individual:

- Racial or ethnic origin
- Political opinion
- Religious belief
- Trade union membership
- Physical or mental health
- Sexual Life
- Commission of offences or alleged offences

Personal data, in all forms, whether electronic or in hard copy, will be held in accordance with the retention guidance to be found in the Record Retention Schedule.

2.3 What/Who is the Data Subject?

The data subject is the individual to whom the information relates

2.4 What/Who is the Data Controller?

The data controller is defined as the person/organisation who either alone or jointly or in common with others determines the purposes for which and the manner in which any personal data are to be processed.

(Employees who process personal data as part of their work for an organisation are part of the data controller function in that they must work according to the organisation's procedures.)

2.5 What is processing?

Data processing is any activity involving personal data. This includes obtaining, recording, transferring, storing, retrieving, consulting, amending, printing, deleting and destroying.

2.6 What is a data processor?

A data processor is any person (other than an employee of the data controller) who processes personal data on behalf of the data controller.

2.7 What is a third party?

A third party is any person/organisation other than the Data Subject, Data Controller, data processor or any other person authorised to process the personal data for the data controller or data processor.

3. Scope

This Policy relates to all personal data created, received or maintained or in any way processed by staff working for the TEN Group organisations in the course of their duties. It further applies to all personal data created, received or maintained by external parties/contractors on behalf of the TEN Group organisations and which are subject to Data Processing Agreements.

The TEN Group Board, all members of staff, students, and contractors are required to ensure that personal data in any media, whether paper, tape or digital, which is processed by or on behalf of the TEN Group, is done so in accordance with the 8 Principles of the Data Protecton Act 1998 (see below).

4. Legal Environment

Data Protection Legislation

Any organisation which processes personal data, has a duty to handle that information with care and diligence and must have in place organisational and technological measures to ensure that personal data is kept secure at all times. In relation to the education sector, the following legislation and guidance is particularly relevant.

The most important piece of data protection legislation affecting educational establishments across the UK is the DPA. The Act outlines the conditions that must be met in order to process personal information and lists 8 Principles which have be observed in the processing of this data.

Other relevant legislation includes

- Privacy and Communications (EC Directive) Regulations 2003 which apply to the use of personal data in direct marketing and other use of electronic communications,
- Computer Misuse Act 1990 which relates to unauthorised access or modification to computers,
- Freedom of Information Act 2000,
- Protection of Freedoms Act 2012 which imposes specific requirements in relation to the biometric information.
- Regulation of Investigatory Powers Act (2000)
- Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000

A summary of some of the key pieces of legislation affecting education establishments is detailed in Appendix 1, together with identification of any relevant supporting guidance along with their particular application in relation to the educational setting.

5. Policy Aims & Objectives

The TEN Group Board seeks to ensure that all processing of personal data undertaken by member organisations of the TEN Group complies with the DPA and this policy recognises the rights and obligations established by the DPA in relation to the management and processing of personal data, namely that personal data is processed in accordance with the **8 Principles of the DPA**, namely:

- Fairly and lawfully processed
- Processed for limited purposes and not further processed in a manner incompatible with those purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the data subject's rights
- Secure
- Not transferred to other countries unless adequate levels of protection are ensured

6. Roles and Responsibilities

6.1 Board of Governors and Principals / Managing Director

The governing body for each organisation within the TEN Group is the Data Controller for their organisation. It has accountability for data protection and for ensuring that measures are in place relating to personal data being fairly, lawfully and securely processed.

The governing body has delegated the responsibility of Data Controller to the Principal or Managing Director.

The Data Controller has responsibility for ensuring the effective management of data protection in all processing. This is implemented via the Heads of School/Department Managers and with the specialist advice and assistance of NES staff. Furthermore, the Data Controller ensures that adequate arrangements exist for the effective implementation of the TEN Group Data Protection Policy; this is achieved through procedures in place.

The Data Controller is responsible for ensuring that the necessary resources are in place to secure full compliance with statutory requirements including the provision of appropriate technological and organsiational measures for the protection of personal data and staff awareness training; and to ensure that adequate resources are made available for data protection purposes; and to ensure organisational arrangements are implemented effectively.

The Data Controller has overall accountability for the strategic direction, oversight, monitoring, and leadership of data protection and is the named person responsible for ensuring that the objectives of the TEN Group Data Protection Policy are achieved.

6.2 All Staff

All staff are responsible for:

- processing personal information fairly, lawfully and securely
- seeking guidance if they believe that personal data may at risk of damage, loss or unauthorised disclosure
- reporting any breach of the DPA
- complying with all data protection requirements
- maintaining their knowledge and understanding of Data Protection, through annual mandatory training

All staff, whether or not they physically create, receive or maintain personal data themselves, have an obligation to comply with the principles and requirements of the DPA.

6.3 Health, Safety & Professional Compliance Team (NES)

The TEN Group Health, Safety & Professional Compliance Team (NES) has a central co-ordinating role in relation to general data protection matters with particular emphasis on the provision of guidance and advice to the Data Controllers within the Group relating to the requirements, interpretation and application of relevant legislation. The Health, Safety & Professional Compliance Manager (NES) has a pivotal role in the development and promotion of the TEN Group's Data Protection Policy, strategic plans and, with the Director of IT Services (NES), the development of effective data protection security across the TEN Group.

The Health, Safety & Professional Compliance Manager (NES) fulfils the following functions:

- oversees the effective implementation of data protection legislation on behalf of the Data Controller
- provides competent advice and guidance to managers and other employees on matters of personal data
- reports to all Data Controllers on data protection performance
- identifies and promotes relevant data protection compliance training for staff at all levels
- promotes a positive professional compliance culture within TEN Group in order to imbed privacy awareness as a norm in all personal data processing
- undertakes monitoring and auditing of professional compliance across the TEN Group.
- develops opportunities for professional compliance shared services with external organisations.

7. Reference to other relevant policies and procedures

TEN Group procedures

Information Security
Records Management/Archiving
Use of Social Media and Networking
Record Retention Schedule
Marketing and Data Protection
Freedom of Information
Audit
Use of Email
Use of Faxes
Use of Personal Images
Clear Desk Guidance
Privacy Impact Assessments

Organisational specific procedures

Data Protection Code of Practice
Student / Staff Conditions of Use of IT Systems
Subject Access Request
Room and Buildings Clearance
Police Requests for Personal Information
Data Security Breach Management
e-Safety
Disposal of Confidential Waste
Handling Complaints
CCTV Monitoring
Research Activity

8. Arrangements for managing data protection

8.1 Monitoring the implementation and effectiveness of the policy

The Health, Safety & Professional Compliance Manager (NES) monitors the effectiveness of this procedure through audit, and acting on reports received, and prepares data incident statistics, statistics relating to Privacy Impact Assessments and information requests as required. The Health, Safety & Professional Compliance Manager (NES) reports monthly to all the Data Controllers and reports recommendations for action if necessary.

8.2 Registration with the ICO

Each TEN Group organisation is registered with the ICO for the personal data processing it undertakes.

8.3 Arrangements for Privacy Impact Assessments

Privacy Impact Assessments (PIAs) are integrated into the planning of all new projects or activities which involve the processing of personal data, the use of new technology related to personal data processing or new arrangements for processing personal data e.g. working off-site. Implications for privacy and data protection are considered at an early stage and the measures to address risks are recorded together with control measures. The Project Leader/Manager responsible for the project or the area of activity undertakes the PIA in consultation with stakeholders and the Health, Safety & Professional Compliance Team (NES).

8.4 Arrangements for Training

To support the implementation of the Data Protection Policy, training is provided for Managers and Staff as required. Additional training needs are identified by PIAs, risk assessments, audits and individual appraisals. Data Protection training is organised by the Health, Safety & Professional Compliance Team (NES) in conjunction with the Human Resources Training & Development Team (NES).

Induction information for all new staff includes information about Data Protection and specifically the TEN Group Data Protection Policy.

Managers and supervisors ensure that staff receive adequate training in data protection and privacy matters.

8.5 Arrangements for Audit

The Health, Safety & Professional Compliance Team (NES) undertake a programme of organisation audits on a regular cycle.

Managers undertake a departmental audit of Data Protection practice using TEN Group Data Protection checklists. Managers record all significant issues identified and any remedial action taken.

8.6 Arrangements for Communication

Information about Data Protection is made available to staff using the Intranet, newsletters and email. Requests for information in alternative formats should be made to the Health, Safety & Professional Compliance Manager (NES).

8.7 Arrangements for Privacy Notices

Principle 1 of the DPA requires that personal data is processed fairly and lawfully. At the point of gathering personal information for processing, data subjects are given information relating to

- the organisation – under the TEN Group each institution is its own data controller.
- the purpose of processing.
- with whom personal information will be shared.

- where relevant, the consequences of not providing information e.g. where individuals are sponsored by their employer.

Managers ensure that hard copy/electronic forms and other technologies which are used to gather personal data are accompanied by Privacy Notices at the point of collection.

8.8 Arrangements for Data Sharing Agreements

Where regular exchange of personal data takes place with another organisation and where each organisation makes decisions relating to the personal data, a Data Sharing Agreement is negotiated. A Data Sharing Agreement is concerned purely with personal data and identifies:

- the legal basis for sharing information
- the responsible post-holders and their delegates
- the purpose of the data sharing
- the specific fields of data to be shared
- the responsibilities of each party in relation to Subject Access Requests, Complaints, Breaches of the DPA
- Retention of personal data
- Security measures
- Termination arrangements

Privacy Impact Assessments identify the need for a Data Sharing Agreement at an early point in planning new activity which involves personal data.

Managers consult the Health, Safety & Professional Compliance Team (NES) where the regular exchange of personal data occurs or is planned.

8.9 Arrangements for Data Processor Agreements

Where a third party processes personal data on behalf of NES, a Data Processor Agreement is negotiated. A Data Processor Agreement is concerned purely with personal data and ensures that:

- Processing of personal data is only undertaken in accordance with instructions from the organisation and in accordance with the DPA
- appropriate security measures are in place to safeguard the personal data from any unauthorised and unlawful processing, accidental loss, damage, alteration or disclosure
- the Data Processor has undertaken reasonable steps to ensure the reliability of personnel with access the personal data
- the specific fields of data to be shared
- arrangements in relation to Subject Access Requests, Complaints, Breaches of the DPA
- Retention of personal data
- Security measures
- Inspection
- Termination arrangements

Privacy Impact Assessments identify the need for a Data Processor Agreement at an early point in planning new activity which involves personal data.

Directors and Managers consult the Health, Safety & Professional Compliance Team (NES) in advance where a third party is to process personal data on the organisation's behalf or as part of a service which it plans to offer.

8.10 Arrangements for Requests for Access to Personal Information

All individuals (staff and other data subjects) have the right of access to personal data which an organisation holds about them. Individuals (or their nominees) need to submit a written request clearly stating what personal data is being requested.

The Health, Safety & Professional Compliance Team (NES) receives and processes requests for access to personal information from data subjects and third parties acting on their behalf. Requests are processed promptly and within 40 calendar days once necessary information and payment is received. Queries relating to such requests received by other staff are referred to the Health, Safety & Professional Compliance Team (NES).

Queries relating to requests for personal information received in relation to the prevention and detection of crime and legal proceedings are also referred to the Health, Safety & Professional Compliance Team (NES) who process these in accordance with the DPA.

8.11 Arrangements for Complaints about the processing of Personal Data

Queries relating to complaints received regarding the processing of personal data must be promptly referred to the Health, Safety & Professional Compliance Team (NES).

Formal complaints must be submitted in writing or by email (to DATA_PROTECTION@ccn.ac.uk) and the organisation is required to respond within 21 days.

8.12 Arrangements for Records Management

Records, including those containing personal information, are subject to the TEN Group Records Management procedure and the TEN Group Record Retention Schedule.

Managers are responsible for the management of records held locally and ensure that information on material that is submitted to the central archive is held in such a way as to enable later retrieval.

The Health, Safety & Professional Compliance Team (NES) oversees the arrangements for material received into and held in the central archive, and liaises with Managers with regards to retrieval, return and destruction.

Requests for the retrieval of archived personal files are subject to a protocol requiring confirmation of the request by a manager.

8.13 Arrangements for Personal Data - Storage

Personal data may only be stored on TEN Group-owned mobile devices which are equipped with appropriate encryption facilities. No personal data belonging to the TEN Group may be stored on personally owned mobile devices.

Whilst staff are processing hard copy personal data care must be taken to ensure that it is kept secure and out of sight when not specifically in use.

Hard copy personal data that is no longer in active use must be retained securely in accordance with the TEN Group Record Retention Schedule.

Requests for submission of hard copy material to the archive must be directed to the Health, Safety & Professional Compliance Team (NES). When teams submit items to the archive they must retain relevant information in a form that is accessible to successor individuals/teams to allow later retrieval.

8.14 Arrangements for Retention and Disposal of Personal Data

Personal data is retained in accordance with the TEN Group Record Retention Schedule

Personal data held in hard copy form is disposed of by using the TEN Group Disposal of Confidential Waste procedure.

The disposal of hardware that may contain personal data in digital form is carried out in conjunction with IT Services (NES).

The Director of IT Services (NES) ensures that measures are in place to safely cleanse all equipment (including Multi-Function Devices) which is owned by the TEN Group or is hired on behalf of any TEN Group organisation.

8.15 Arrangements for Reporting Personal Data incidents

A breach of the DPA occurs when personal information is not processed according to the 8 Principles of the Act and may include loss, damage, theft or disclosure to an unauthorised third party.

A member of staff who believes that there may have been a breach of the DPA, must notify their Manager.

Managers who are advised that a data incident may have or has occurred should notify the Data Controller and the Health, Safety and Professional Compliance Team (NES). The Health, Safety and Professional Compliance Team (NES) will assist with an investigation of the incident and where necessary will make recommendations for action.

The Data Controller will decide on notification of any breach to the ICO.

8.16 Arrangements for Room and Building Re-assignments

Managers are responsible for ensuring that hard copy personal data stored in a staffroom or classroom which is under their remit, and which is to be vacated, is appropriately managed and prepared for transfer. They are also responsible for ensuring appropriate communication with Campus Services (NES) up to and beyond the point of transfer.

Staff who occupy a staffroom or classroom in which hard copy personal information is stored and which is to be vacated, are responsible for ensuring that the personal data is appropriately prepared and boxed securely in sealed boxes which are labelled with Staff/Team Name, date of boxing, and future location details.

NES Campus Services (NES) must be notified of the details relating to the number of boxes, the staff/team name associated with them, their current location, and the location to which they are to be transferred.

At the earliest opportunity after transfer, the responsible Manager confirms with NES Campus Services (NES) that the boxes have been received in the appropriate locations.

8.17 Arrangements for Staff Leavers/Transfers to new Role

When an existing member of staff leaves or transfers to a new role within the organisation or the TEN Group, Line Managers are responsible for ensuring that relevant personal data, particularly in hard copy form, is accounted for. The personal data is either appropriately re-allocated to a new responsible person, or is archived or destroyed as appropriate to the circumstances.

When a member of staff leaves the organisation, the Staff Leaver procedure is invoked by Human Resources Services (NES).

Staff leaving the organisation must not, on leaving, retain personal data belonging to any TEN Group organisation. Staff are required to surrender Staff ID cards and door keys and cards giving access to secure areas.

8.18 Arrangements Clear Desk Practice

Teams involved in processing large volumes of personal data or small amounts of sensitive personal data are required to keep desks clear in accordance with the Clear Desk Guidance. To limit the risk of paper records being lost, stolen, inappropriately accessed or damaged, desks are cleared of any confidential or personal information when the user leaves the office.

Where available, paper records are stored in suitable locked safes, cabinets or other secure furniture when not in use. Where lockable furniture is not available, doors to the office are secured. Keys or codes used to lock away records are not left on display, and are locked in a key cabinet where available.

Visitor, appointment or message books are locked away when not in use.

Computers, laptops and other devices used to process personal data are not left so that information is accessible when unattended, and are protected by passwords.
Access passwords are not written down or available to others under any circumstances.
Screens are locked when computers are left unattended, irrespective of the amount of time spent away.

Computer screens are positioned away from the view of visitors or the public, and angled away from windows or open areas. Where it is not possible to position screens out of sight, a privacy screen filter will be used.

8.19 Arrangements for the Use of Email

Email as a means of communication is particularly vulnerable to breaches of the DPA. Staff apply the guidance given in the Good Practice guide on the use of Email.

Email is not used to communicate personal data unless the data is encrypted. Guidance should be sought from IT Services (NES) where encryption may be needed.

8.20 Arrangements for the Use of Fax

Fax as a means of communication is particularly vulnerable to breaches of the DPA because of the risk of inputting an incorrect number. Staff must apply the guidance given in the Good Practice guide on the use of Fax.

Fax is not used to communicate personal information. However, if deemed necessary in cases of sufficient weight and extreme urgency (and only where encryption for email is not available), it may be used but only according to the guidance given.

8.21 Arrangements for Purchasing

Before requesting or purchasing equipment relating to the storage and processing of personal data (e.g. mobile devices, surveillance equipment etc.), departments consider any risks to privacy and consult both IT Services (NES) and the Health, Safety & Professional Compliance Team (NES) who will be able to advise with regard to encryption, destruction and legislation.

8.22 Arrangements for Marketing

The DPA provides individuals with the right to prevent processing of their personal data for direct marketing purposes.

Managers are responsible for ensuring that any marketing exercise in which they participate is undertaken lawfully and that the requirements of both the DPA and the Privacy & Electronic Communications (EU Directive) Regulations 2003 are observed.

8.23 Arrangements for Social Media and Networking

Use of social networking applications as part of a service provided by the organisation or the TEN Group (whether they are hosted by the TEN Group or by a third party) is facilitated by the New Media Team who monitor subsequent use. Staff must not post personal images of others without explicit, fully informed consent.

Whether acting on behalf of the organisation/TEN Group or in a private capacity, staff do not publish or disclose any private, personal or confidential information obtained at work, including information relating to staff, customers, service users or other third parties with whom they come into contact.

Staff who are involved in recruitment do not seek, through the internet, further information about candidates beyond that which candidates have provided as part of their application.

8.24 Arrangements for Visitors

Visitors are responsible for any personal data which they carry whilst on the organisation's premises and must not dispose of hard copy material containing personal data which is in their possession in the organisation's waste facilities.

8.25 Arrangements for Contractors

Contractors working on sites belonging to the TEN Group are asked to notify Campus Services (NES) should they be exposed to personal data during the course of their work.

Contractors are responsible for any personal data which they carry whilst on the premises and must not dispose of hard copy material containing personal data which is in their possession in the organisation's waste facilities.

Appendix 1 - Relevant legislation

Data Protection Act 1998

Primary legislation for data protection in the UK. Enforced by the ICO and details the statutory requirements for processing personal data.

Identifies the 8 Principles under which all personal data must be processed, includes the sanctions that apply in the event of a breach and misuse of personal information by individuals.

A breach of any of the other Principles of the DPA automatically invokes a breach of the First Principle that personal information must be processed fairly and lawfully.

Privacy & Electronic Communications (EC Directive) Regulations 2003

These regulations relate to direct marketing and make it unlawful to send someone direct marketing who has not previously given specific permission for their personal information to be used in this way (unless a previously existing relationship exists between the parties).

Freedom of Information Act 2000

This statutory legislation places a requirement on all public bodies to manage records in such a way as to ensure that information is retained only as long as necessary and in such a way that it is identifiable and retrievable.

Protection of Freedoms Act 2012

The Protection of Freedoms Act

- places a requirement on data controllers in Schools and Colleges to obtain parental consent for the gathering of biometric data.
- Regulates the use of CCTV for surveillance purposes.

Computer Misuse Act 1990

The purpose of this legislation is to secure computer material against unauthorised access or modification and for connected purposes; hacking and the introduction of viruses are criminal offences under this legislation.

Regulatory of Investigatory Powers Act 2000

This legislation limits and sets out circumstances in which individuals can be subjected to various forms of covert surveillance including telephone tapping, interception of correspondence and covert filming e.g. use of CCTV.
It specifically provides that the interception of private communications is unlawful other than where interception takes place in accordance with the provisions of the Act.

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

This legislation permits a business to intercept communications on its own network email and internet abuse and to record telephone conversations to evidence transactions