TEN Group Data Protection Policy

Policy number:	DP01
Version:	2.5
Policy holder:	Head of Professional Services
Approval board:	TEN Group CEO
Date of approval:	May 2018
Review period[1]:	24 months
Date of latest review:	May 2018
Target review date[1]:	May 2020
Legislation or regulation:	• General Data Protection Regulation • Privacy and Communications (EC Directive) Regulations 2003 • Computer Misuse Act 1990 • Freedom of Information Act 2000 • Protection of Freedoms Act 2012 • Investigatory Powers Act (2016) • Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000

[1] The Review Period and the Target Review Date refer to our internal policy review process. The published policy is current and is the most recent approved version

Version Control Document

Date	Version No.	Reason for Change	Author
January 2017	2.0	Rewrite / Incorporate GDPR	Dawn Clarke
May 2017	2.3	Review	Peter Beacock
November 2017	2.4	Contact number updated	Peter Beacock
May 2018	2.5	Updated to reflect changes in legislation/regulation	Peter Beacock

Contents

1. Policy Statement

The TEN Group is committed to fostering high standards of data protection in all processing of personal data relating to the Group's employees and pupils/students, contractors and visitors. In particular, the TEN Group will work to ensure that all legal obligations under the General Data Protection Regulation (GDPR) and successor legislation are met by all organisations.

The TEN Group Board & Group Chair actively promotes a culture whereby the principles of the GDPR 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.

2. Policy Aims & Objectives

This policy aims to explain the requirements of the legislation, sets out the expectation for compliance, and signpost relevant procedures and guidance notes to support staff.

The policy sets out the following objectives for all organisations within the TEN Group:

- ensure that personal data is processed fairly and lawfully, and only for specified purposes, using an information asset register to record processing activities;
- allocate specific responsibilities for data protection compliance;
- 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 adequate notification and communication to staff and pupils/parents or students on the processing of their personal data;
- ensure appropriate procedures are in place to respond to individuals who are exercising their rights under relevant legislation;
- provide adequate information instruction and training for staff who are processing/handling personal data;
- ensure any incidents or breaches involving personal data are recorded, investigated and, where appropriate, reported to the regulator;
- provides adequate resources to deliver secure processing of personal data undertaken at any of their managed sites or at any other workplace.

3. Definitions

3.1 Personal Data

The GDPR defines personal data as information that:

- Identifies[1] a living individual;
- is stored and used electronically, or within structured manual records, and includes accessible records such as education or health records;
- includes an expression of opinion about or intention towards a person.

- Personal Data that has been pseudonymised – eg Key-Coded – can fall within this scope depending on how difficult it is to attribute the pseudonym to a particular individual is.

[1] The individual can be identified from the information itself, i.e. it includes their name, or when linked with other information that we hold, e.g. under a unique reference number.

3.2 Sensitive personal data (Special Category)

The GDPR refers to sensitive personal data as "special categories data" and specifies this data as:

- Racial or ethnic origin
- Biometric data
- Genetic data
- Political opinion
- Religious or similar beliefs
- Trade union membership
- Physical or mental health
- Sexual Life
- Commission of offences or alleged offences

This type of data is subject to further regulation under GDPR and can be processed only under certain circumstances.

3.3 Processing

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

3.4 Data Subject

The individual to whom the information relates.

3.5 Data Protection Officer (DPO)

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring the TEN Group and its organisations compliance with data protection law, and developing related policies and guidelines where applicable.
The DPO is also the first point of contact for individuals whose data the TEN Group and its organisations processes, and for the ICO.

3.6 Data Controller

The person/organisation who, either alone or jointly or in common with others, determines the purposes and manner of the processing of personal data. This is usually the organisation, company etc which is the controlling legal entity. Functions can be delegated to senior designated individuals.

In the TEN Group each governing body/board is a Data Controller for their organisation. The Norfolk Academies Trust has overarching responsibility as Data Controller for the Academies within the Trust.

3.7 Data Processor

Any person (other than an employee of the Data Controller) who processes personal data on behalf of the Data Controller.

In the TEN Group, NES is a Data Processor contracted to carry out functions for the rest of the Group and therefore processing personal data on behalf of those organisations. NES is also a Data Controller when it processes personal data for its own purposes, e.g. management of NES employees.

3.8 Third Party

Any person/organisation external to the TEN Group's trustees, employees, and the data subjects.

4. 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.

5. Legal Requirements

General Data Protection Regulation (GDPR)
This is the primary legislation covering personal information. The GDPR requires that the processing of personal data complies with all of the principles specified under Article 5 of the GDPR, as follows:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

Other legislation creates additional requirements relating to types and/or processing activities of personal data:

- 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, which provides for access to all information held by public authorities;
- 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

Legislation relating specifically to education also has implications for the processing of personal data. Further information is available at Appendix 1.

6. Procedure

6.1 Monitoring the Implementation and Effectiveness of the Policy

The Head of Professional Services and the Information Compliance Team 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 Head of Professional Services reports monthly to all the Data Controllers and reports recommendations for action if necessary.

6.2 Registration with the ICO and the Data Protection Fee

Each TEN Group organisation is registered with the Information Commissioner's Office for the processing of personal data, with renewals managed by the Information Compliance Team. Organisations will inform the Information Compliance Team of any changes to processing activities so the registration can be updated as necessary.

The requirement to register will be removed under GDPR. Organisations will be required to pay the ICO a data protection fee unless they are exempt. The new data protection fee replaces the requirement to 'notify' (or register), which was covered by the Data Protection Act 1998. The ICO have the power to enforce the 2018 Regulations and to serve monetary penalties on those who refuse to pay their data protection fee.

6.3 Privacy by Design / Privacy by default

The TEN Group have measures in place to show that the Group and its organisations have integrated data protection into all of their data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in the GDPR
- Completing Privacy Impact Assessments (PIAs) where the organisations process of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Developing IT systems, services, products and processes that involve processing personal data
- Developing organisational policies, processes, business practices and/or strategies that have privacy implications
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the contact details of the TEN Group DPO and all information the Group is required to share about how they use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party

recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

6.4 Privacy Risk Assessments

Privacy Risk Assessments (PIAs) are a form of risk assessment and a process for undertaking a PIA based on the standard risk assessment process for health and safety risks is shown at Appendix 3. As a requirement of the GDPR, PIAs will be 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 privacy risk assessment in consultation with stakeholders and the Information Compliance Team.

6.5 Staff Training and Awareness

TEN Group Induction sessions for all new staff includes information about data protection and the handling of personal information. Under local induction arrangements, staff are issued with a copy of the Data Protection Good Practice Guide.

All staff are required to complete mandatory Data Protection Core Training, via an online module or a one hour session delivered by the Information Compliance Team, with the training repeated every two years. Principals and managers are responsible for ensuring that staff complete the training and have sufficient time allowed. The NES Training and Development Team monitor completion figures and report to Principals/Managers on a regular basis. Staff who fail the end of course test twice or more are referred to the Information Compliance Team for additional training. Persistent failure to pass the training may be dealt with as a performance issue: persistent failure to undertake the training will be dealt with as a disciplinary matter.

Additional and bespoke training sessions can be provided by the Information Compliance Team on request, and as identified via PIAs, audits and staff development needs analysis. Information about data protection compliance measures is made available to staff using the Intranet, newsletters, and awareness poster campaigns. Requests for information in alternative formats should be made to the Information Compliance Team.

6.6 Audit

The Information Compliance Team undertakes audits of each organisation's compliance with the legislative requirements and this policy. Following an audit, an action plan for improvement is developed and agreed with the organisation.

6.7 Privacy Notices and Communication to Data Subjects

Privacy notices and communication with data subjects about how their personal data is being processed is a requirement under Articles 12, 13, 14, 15 to 22 and Article 34 of the GDPR. The Information Compliance Team produces a privacy notice for each organisation, which is published on websites and can be issued with Admissions Forms or at other appropriate points when information is being collected. A privacy notice contains the following information:

- details of the Data Controller;
- all purposes for processing of personal data;
- with whom personal information will be shared.

- The rights of the data subject in relation to their personal data

New arrangements to collect and/or use personal data will require additional notification to data subjects and amendment to the published privacy notice. Managers are to 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.

Privacy notices relating to the processing of staff personal data are published on the Policy Portal.

Privacy notices should be in a format and style appropriate for the audience, particularly to ensure they are easily understood by the various age groups of our students.

6.8 Lawful Processing, Consent and Right to Erasure ('right to be forgotten')

Lawful Processing
The primary function of the organisations within the TEN Group is that of education, either as a provider or in support of the providers. In order for the use of personal data to be lawful, the purpose should relate to:

1. a legitimate and justified function of an educational establishment, and
2. the articles of corporation or funding agreement for the establishment, and
3. meet a condition for processing established by Article 6 (and Articles 9 and 10 where necessary) of the GDPR.

Consent
Where the purpose for using personal data does not fall within points 1 and 2 above, and there is no legal obligation for the processing, it may be necessary to obtain consent from the individual(s). Consent should be obtained only when it can be given freely, and be equally freely withdrawn without causing detriment to the individual. Consent should not be used purely as a 'safety net' to legitimise the processing, but only when there is no other justification for the processing.

Under the GDPR the use of consent attracts additional rights, including the right for all data to be deleted when consent is withdrawn, and therefore it will be important to ensure it is used only when appropriate.
Where online services are made available to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will seek parental consent (except for online counselling and preventive services).

Right to Erasure ('right to be forgotten')
Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;

- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the GDPR.

6.9 Limitation, minimisation and accuracy

The organisation will only collect personal data for specified, explicit and legitimate reasons. These reasons are explained when data is initially collected.

If the organisation wishes to use personal data for reasons other than those given when first obtained, they will inform the individuals concerned before they do so, and seek consent where necessary.

TEN Group staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the organisations records management retention schedule.

6.10 Use of Personal Images, Photographs and Videos

Photographs and images of people can capture the distinguishing features of an individual which identify them. The organisation will also have information such as name etc. which they can link to the image to enable further identification. Images can also be capable of being sensitive personal data, for example, if they can depict a person's racial or ethnic origin, or show that a person has a disability.

The taking, using and sharing of personal images will be handled in accordance with Article 5 of the GDPR in the same way as other types of personal data. Students, staff and others must be informed of when and why personal images might be taken and/or used, and ask for consent when use of the image is for a purpose not specific to the individual's education and is not covered by the organisation's privacy notice.

The TEN Group does not advocate a policy of a blanket ban of the taking of images by parents/carers etc. as a family record of their child's participation in school/college life. It will be for each organisation to decide on their approach locally, and this can be adjusted depending on the event and the students involved. It is expected that restricting parents/carers from taking images will be on an exceptional basis and in relation to specific, identified safeguarding needs. If restrictions are to be in place these are to be notified to visitors as soon as possible.

Further information is available in the Use of Personal Images Guidance Note published on the Policy Portal.

6.11 Closed Circuit Television (CCTV)

Closed Circuit Television (CCTV) is widely used in the UK to enhance safety and security. The presence of CCTV can act as a deterrent to those intent on committing crime or other inappropriate behaviours against others or property, and communities can feel safer as a result. Images recorded by CCTV can be significant in the investigation and resolution of incidents, sometimes providing an unequivocal portrayal of events. However, it is accepted that CCTV is intrusive, providing an ongoing record of individuals' movements and activities. The usefulness of CCTV images can be much reduced by poor siting of equipment, and poor quality. For this reason, the TEN Group has put in place requirements on all of its organisations to ensure the use of CCTV is fully and properly assessed, implemented and monitored in accordance with relevant legislation and codes of practice.

Organisation in the TEN Group use CCTV only for the following purposes:

- To detect, prevent or reduce the incidence of crime
- To prevent and respond effectively to all forms of harassment (including bullying) and disorder
- To improve communications and the operational response of security patrols in and around the areas where CCTV operates
- To reduce the fear of crime
- To create a safer community
- To gather evidence by a fair and accountable method
- To provide emergency services assistance
- To provide assistance for internal investigations/disciplinary hearings within the institution for the purpose of safety and security of all campus users and their property.

With regard to internal investigations/disciplinary hearings, CCTV images will be used only when the alleged conduct is classed as 'gross misconduct' according to the organisation's employee and student conduct policies and the alleged conduct is deemed to have compromised the safety and security of individuals or property. For incidents not relating to gross misconduct, CCTV images can be used only with the consent of all relevant parties.

CCTV systems will not be used to monitor the performance of employees without their knowledge.

If any organisation wishes to change the use it makes of CCTV, it must contact the Information Compliance Team so that arrangements are made to amend the notification.

Organisations using CCTV will ensure the following is in place:

- A Privacy Impact Assessment has been conducted for any new/changed use
- The statutory notification to the ICO and the published Privacy Notice states that CCTV is in use and specifies the purpose(s) of its use
- A staff member is nominated as CCTV Manager and has responsibility for the operation of the CCTV system
- The Information Compliance Team is consulted and a CCTV Code of Practice is put in place

Further information is available in the CCTV Guidance Note and CCTV Code of Practice Template published on the Policy Portal.

6.12 Use of Biometrics

Organisations within the TEN Group can opt to use biometric data for the purpose of cashless catering, printing, IT access, library services and similar activities where a transaction needs to relate directly to the individual.

There are legal requirements to follow when introducing biometrics, set out in the Protection of Freedoms Act 2012. Biometric information is also defined as special category personal data and all the usual provisions of the GDPR will apply. The DfE has published guidance which contains full details of how the biometric data of children is to be handled by educational establishments.

This paragraph taken from the legislation states clearly the overriding requirement when introducing biometrics:

> There will never be any circumstances in which a school or college can lawfully process a child's biometric information (for the purposes of using an automated biometric recognition system) without one of the persons [with parental responsibility] having given written consent.

The Use of Biometrics Guidance Note published on the Policy Portal sets out the consent process that must be undertaken when using biometric data.

6.13 Personal Data and Social Media

Sharing an individual's personal data via social media (e.g. Twitter, Facebook etc) places that information in the public domain and it can be re-shared/retweeted multiple times and reach a huge audience. Care must be taken when using personal information in this way and, as well as ensuring any such use of personal data complies with the GDPR, staff should refer to the TEN Group Social Media Policy for guidance.

6.14 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 and purpose for the data sharing
- a description of the data to be shared
- the responsibilities of each party in ensuring compliance with the GDPR
- security measures
- termination arrangements

Managers are to consult the Information Compliance Team where the regular exchange of personal data occurs or is planned. Further information is available in the Personal Data Disclosure Guidance Note available on the Policy Portal.

6.15 Data Processor Reviews and Agreements

Where a third party processes personal data on behalf of a TEN Group organisation, a review of the third party data protection compliance arrangements is undertaken by the Information Compliance Team, and, where appropriate, 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 GDPR

- 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
- arrangements in relation to Subject Access Requests, Complaints, Breaches of the GDPR
- termination arrangements, including the disposal of the personal data

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 are to consult the Information Compliance Team 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. Further information is available in the Disclosure of Personal Information Guidance Note available on the Policy Portal.

6.16 Third Party Requests for Disclosure of Personal Data

Where ad hoc requests from third parties for the disclosure of information about an individual are received, these are not processed unless the request is in writing and one of the following applies:

- the condition(s) for processing have been met, e.g a legal obligation, a contract, consent etc
- an exemption applies

In many cases, the consent of the data subject should be obtained. However, if the disclosure is required under a legal obligation, or an exemption is relevant, consent is not appropriate. Consideration should be given whether to notify the data subject(s) of the proposed disclosure, unless this would prejudice the purpose for the disclosure.

In some circumstances, a fee may be charged for the provision of information. A 'reasonable fee' can be levied for the administrative costs of complying with the request. The TEN Group Policy covering the Charging of Fees for the Provision of Information (Statutory Requests) is available on the Policy Portal.

Disclosure of personal data to third parties is a complex area and all such requests are to be notified to the Information Compliance Team who undertake the response to the request on behalf of the receiving organisation, or will provide advice. Further information is available in the Disclosure of Personal Information Guidance Note available on the Policy Portal.

Where there is a regular and routine need to share information between organisations, a Data Sharing Agreement is needed. (See item 6.7)

6.17 Subject Access Requests

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) can make the request verbally or in writing but must clearly state what personal data is being requested.

The Information Compliance Team receives and processes subject access requests on behalf of all organisations in the TEN Group. Requests are processed promptly and within one calendar month once necessary information is received.

6.18 Professional Content

The legal definition of personal data includes 'expressions of opinion about the data subject, and intentions towards them' and information recorded in any format, including notes and emails. All information recorded about individuals will be professional in tone and content, and will be accurate as far as is possible depending on the source of the information.

6.19 Complaints, Incidents and Breaches Involving the Processing of Personal Data

A breach of the GDPR (or other related legislation) occurs when personal information is not processed according to Article 5 and may include loss, damage, theft or disclosure to an unauthorised third party. In most cases a breach will result in a data subject suffering detriment, including a breach of their privacy and of their expectations of how their personal information will be handled, as well financial or other tangible loss.

A data processing incident refers to processing that may not meet the requirements of the legislation and/or TEN Group policy but has not resulted in actual loss, damage or unauthorised disclosure of personal data or, if such loss etc has occurred there has been no detriment to the data subject. An incident will generally come to light through employees self-reporting.

Complaints about the handling personal data can be made by any person whose information is held by any organisation in the TEN Group and will be dealt with under the relevant organisation's Complaints Policy and Procedure, with the advice of the Information Compliance Team. Staff who believe their personal data may have been handled inappropriately can report this to their manager, direct to the Information Compliance Team, or can refer to the TEN Group Grievance Policy and Procedure.

A member of staff who believes that there may have been an incident or breach or is in receipt of a complaint, must notify their Manager.

Managers who are advised of an incident, breach or complaint, must notify the Data Controller and the Information Compliance Team. The Information Compliance Team will assist with an investigation of the matter, will, where appropriate, make recommendations for action and rectification, and will assess and advise whether a breach of the relevant legislation has occurred. The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (ICO). This must be completed within 72 hours of becoming aware of the breach, where feasible.

Where it is suspected that the actions/conduct of a member of staff has led to a breach of the GDPR, or other related legislation, consideration will be given to whether the matter should be dealt with under the TEN Group Disciplinary Policy. Depending on the severity of the breach, the conduct may fall under the definition of Gross Misconduct outlined in that Policy.

Staff who have intentionally or negligently ignored TEN Group policy, procedures and training relating to the handling of personal data may be subject to a criminal investigation and proceedings.

6.20 Records Management

Records, including those containing personal information, are subject to the TEN Group Records Management Policy and the relevant Record Retention Schedule (Academies & UTCN/CCN) published on the Policy Portal. It is important to ensure that information, particularly personal information, is stored and logged in such a way that it can be located and retrieved at a later date is required for business reasons, and in order to comply with legal requirements such as responding to a subject access or Freedom of Information Act request.

Each organisation is responsible for the secure and accessible storage of records locally, and for ensuring their secure disposal at the appropriate time.

The Information Compliance Team oversees the arrangements for records stored in the central archive at City College Norwich and in commercial off-site storage.

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

6.21 Secure Storage and Handling of Personal Data

As well as the general guidelines issued under induction and core training, all staff receive training on appropriate local security arrangements for the type of personal data they will handle in the course of their role. This will include arrangements for:

- clear desk practice
- suitable secure storage
- locking screens when unattended, and the siting of screens/use of screen filters so information is not visible to others
- permission-based electronic storage
- secure sharing and transmission of information, using secure networks, cloud-based sharing, and encryption tools
- issue of TEN Group-owned mobile devices equipped with appropriate encryption facilities. No personal data belonging to the TEN Group may be stored on personally owned mobile devices.

For more information about the security of information, please refer to the TEN Group Information Security Policy published on the Policy Portal, or contact IT Services or the Information Compliance Team.

6.22 Disposal of Personal Data

Personal data held in hard copy form is disposed of as Confidential Waste, using the appropriate bins/sacks and in accordance with the TEN Group Disposal of Confidential Waste Guidance Note and related local arrangements.

The disposal of hardware that may contain personal data in digital form is carried out by IT Services in accordance with the Information Security Policy.

6.23 Room and Building Re-assignments

Moving work locations introduces the risk of incidents where personal data has been mishandled, either transported insecurely, lost in transit, left behind, or disposed of inappropriately. Managers and staff are responsible for ensuring that hard copy personal data stored in a staffroom, classroom or office which is under their remit, and which is to be vacated, is appropriately managed and prepared for transfer, including:

- personal data is to be transported in sealed boxes labelled with the owner and destination
- a sweep is to be made of the vacated room, including in, under and behind any cupboards, cabinets etc
- any personal information is disposed of securely (see 6.20).

Organisations may establish their own local procedures for ensuring room/building moves are managed correctly.

6.24 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, the Line Manager is responsible for ensuring that relevant personal data (hard copy and digital) prepared and held by the staff member is accounted for. The personal data must be re-allocated to a new responsible person, be stored in an appropriate shared access area, 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). Local procedures are available on the relevant organisation's area on the Policy Portal.

Staff leaving the organisation must not retain or copy any 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 and any issued IT equipment.

Managers must ensure that, particularly when a staff member moves to another role within the TEN Group, their access to any systems, databases, shared data storage areas, and physical locations is revoked.

6.25 Use of Email

Email as a means of communication is particularly vulnerable to breaches of the GDPR where emails containing personal data are sent to a wrong recipient, are sent over non-secure internet connections, or contain information (often in a chain of emails) that is not appropriate for all recipients. Depending on the sensitivity of the data (personal or otherwise) being transmitted via email, measures should be taken to protect the content, including anonymising (e.g. replace full names with initials), password protecting attachments, and using encryption tools.

Further information is available in the TEN Group Handling Email Guidance Note available on the Policy Portal.

6.26 Use of Fax

Fax as a means of communication is particularly vulnerable to breaches of the GDPR because of the risk of inputting an incorrect number and lack of awareness of the location of the receiving fax machine, which may be in an open office or shared between offices, departments and even businesses.

As a general rule Fax is not used to communicate personal information. However, if deemed necessary in cases of sufficient weight and urgency (and only where encryption/password protection for email is not available), it may be used but measures should be taken to minimise the risk, including:

- contacting the recipient to confirm the fax number
- double checking the input of the number is correct
- checking with the recipient the location of the receiving machine and arranging for the recipient to be at the receiving machine when transmission occurs
- checking with the recipient that the fax has been received in full.

6.27 Purchasing of Equipment or Software for Processing and Storing Personal Data

Before requesting or purchasing equipment or software for the storage and processing of personal data (e.g. mobile devices, surveillance equipment, internet-based services etc.), organisations must consider any risks to privacy and consult both IT Services and the Information Compliance Team for advice about security, encryption, and the suitability of the

product for the purpose. The TEN Group will require systems and software products to incorporate the principle of 'privacy by design' to ensure they are fit for purpose under the GDPR.

6.28 Marketing

The GDPR 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 GDPR and the Privacy & Electronic Communications (EU Directive) Regulations 2003 are observed.

The Information Compliance Team can provide further advice covering:

- ensuring any marketing exercise is covered by the existing privacy notice and notification to the ICO, and arranging an update if necessary
- where the marketing involves data collected directly by the organisation, e.g. current student and/or parent details, they are notified of the intention to send them marketing information and given the opportunity to refuse their consent

6.29 Contractors & Visitors

The conduct of contractors (particularly those that are not supervised) is covered in the Site Rules and includes requirements for confidentiality and compliance with data protection legislation. Visitors to and contractors working on sites belonging to the TEN Group are asked to notify Estates and Facilities should they have unauthorised access to personal data during the course of their visit/work, e.g. screens left unlocked, hard copy not put away.

Visitors and contractors are responsible for any personal data which they bring on to the premises.

7. Organisational Responsibilities

7.1 Governing Body / Board of Trustees / Principals & Senior Management

The governing body/board for each organisation within the TEN Group is the Data Controller for their organisation. The Norfolk Academies Trust has overarching responsibility as Data Controller for the Academies within the Trust. The Data Controller has accountability for data protection and for ensuring that measures are in place relating to personal data being fairly, lawfully and securely processed.

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.
This is designated to the Principals, Heads of School and Department Managers and with the specialist advice and assistance of NES staff.

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 security of personal data and staff awareness training, and to ensure organisational arrangements are implemented effectively.

7.2 Norfolk Educational Services Ltd (NES)

NES is a Data Controller for personal information relating to staff in its employment.

NES is a Data Processor, acting on behalf of and under contract to the educational and governance organisations within the TEN Group in the processing of personal data for a range of purposes. A Data Processing Agreement exists between each organization and NES for this processing.

NES, specifically the Information Compliance and Policies Team in Professional Services, is responsible for providing accurate and appropriate advice and guidance to all organisations in the TEN Group on the measures required to deliver compliance with the GDPR and other relevant legislation.

7.3 All Staff

All staff are responsible for:

- processing personal information fairly, lawfully and securely
- seeking guidance if they believe that personal data may be at risk of damage, loss or unauthorised disclosure
- reporting any incidents and/or breaches of the GDPR
- complying with all data protection requirements
- maintaining their knowledge and understanding of data protection, through bi-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 GDPR.

7.4 The Information Compliance and Policies Team

The Information Compliance and Policies Team in the Professional Services Department 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 Head of Professional Services 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, the development of effective data protection security across the TEN Group.

The Head of Professional Services 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 data protection compliance culture within TEN Group in order to imbed privacy awareness as a norm in all personal data processing
- undertakes monitoring and auditing of data protection compliance across the TEN Group.
- develops opportunities for professional compliance shared services with external organisations.

7.5 Director of IT Services

The Director of IT services is responsible for the management of security measures to protect personal data in all formats including electronic, images, and paper copy.

The Director of IT Services will

- ensure that the appropriate technical measures are in place to protect personal data gathered, stored and transmitted via electronic means from unauthorised access and disclosure; and will provide advice and guidance on the appropriate level of physical security measures to protect personal data in other formats
- liaise with the Head of Professional Services and the Information Compliance Team to ensure consistency of advice on information security measures and the content of training and awareness campaigns
- notify the Information Compliance Team of any projects, procurement and new processes involving personal data, and of any amendments or proposed changes to existing processing activities, and assist with the privacy risk assessment.

8. Reference to other relevant policies and procedures

TEN Group policies, procedures and guidance

Policies
Information Security Policy
Records Management Policy
Social Media Policy
Freedom of Information Policy
Charging of Fees for the Provision of Information (Statutory Requests) Policy

Procedures and Guidance
Data Protection Good Practice Guide (issued to all staff on induction)
Record Retention Schedules
Marketing
Disclosure of Personal Data and Request Handling
Use of Email
Use of Personal Images
Disposal of Confidential Waste
Student / Staff Conditions of Use of IT Systems
Room and Buildings Clearance
CCTV Management and Code of Practice
Use of Biometrics

9. Contact

For further information about any aspect of this policy contact in the first instance the Information Compliance Team on 01603 773585 / 3176 or email data_protection@ccn.ac.uk

10. Equal Opportunities Statement

This policy and procedure has been assessed against the nine protected characteristics outlined in the Equality Act 2010 and no apparent disadvantage to equal opportunities has been determined.

If you have any comments or suggestions in relation to equal opportunities of this policy or procedure please contact the policy holder.

Appendix 1 Relevant Legislation

General Data Protection Regulation (GDPR)

The GDPR (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

The GDPR details the statutory requirements for processing personal data. The Regulation includes the sanctions that apply in the event of a breach and misuse of personal information by individuals, including a criminal offence for disclosure of personal data which is unauthorised and carried out wilfully or negligently.

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). NB. There have been amendments to these regulations in 2004, 2011 and 2016.

Freedom of Information Act 2000 (FOI)

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. The Act also allows any person to request any information held by a public authority. It is important to note that the Act applies only to certain parts of the TEN Group; more information is available in the TEN Group FOI Policy.

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.

Investigatory Powers Act 2016

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 for business purposes and to detect email and internet abuse and to record telephone conversations to evidence transactions.

Education Specific Legislation and Statutory Guidance

There is a variety of legislation which creates either explicit or implied legal powers to collect, use and share personal data. (NB. this list is not exhaustive).

The Children Act (various dates)
The Education Act (various dates)
Education(Pupil Information)Regulations 2005 & 2008
Education(Individual Pupil Information)(Prescribed Persons) Regulations 2009
Education (Parenting Contracts & Orders) Regulations
Education(Penalty Notices) Regulations
Education & Skills Act
Education(Pupil Registration) Regulations
The School Discipline (Pupil Exclusions and Reviews) (England) Regulations 2012
Various Department for Education Statutory Guidance

Appendix 2 Risk Assessment of Personal Data Privacy Impact

Where an activity meets the criteria at 1A below OR the activity involves the use of personal data AND an answer to <u>any</u> of the Screening Questions at 1B is YES, contact the Professional Services Team who will assist you in fully identifying and understanding the privacy impact risk and completing steps 2-5.

1 Identify if an activity might have an impact on privacy & personal data rights

1A. If the project/activity relates to any of the following, a Privacy Impact Risk Assessment MUST be conducted:

- CCTV
- Biometrics (e.g. fingerprint, retina scan)
- Involves High Risk data (see Annex A)

1B. Screening Questions (All questions must be answered)	**YES or NO**
The project/activity involves the use of personal information? (This includes even basic information such as name and Academy/College email address)	YES
Are you collecting or using information about individuals for a new purpose?	
Will the project/activity involve the collection of new personal information about individuals? (i.e. types of data the institution has not previously recorded, or about a group of individuals not previously involved)	
Will the project/activity <u>require</u> individuals to provide information about themselves? (i.e. will individuals have a choice of whether or not to provide the information?)	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? (This will include partnership arrangements with another organisation, requests from local authority/government agencies, providing data for a software service hosted online or by a third party)	
Does the project/activity involve you using new technology that might be perceived as being privacy intrusive? (For example the use of biometrics, moving an existing process online, filming/recording individuals)	
Will the project/activity involve using data to make decisions or take action about individuals in ways that have a significant impact on them? (For example, using performance data to decide on salary increases)	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? (For example, health records, criminal records or other information that people would consider to be private?)	
Will the project require you to contact individuals in ways that they may find intrusive? (For example, using personal contact details)	

Having decided that a PIA is required, use the form at Annex B to carry out and record the assessment.

2 Identify Who is Likely to be Affected

This can include students, staff, parents/family members, staff in other TEN Group institutions, staff from external organisations (e.g. partner agencies, contractors), the public.
The age of students can be a factor, and also mental capacity to understand their rights and how the proposed activity might affect their rights. Children, young adults, and individuals with impaired mental capacity are deemed to be more vulnerable to the impact of a breach of their privacy and personal data rights. In extreme cases, allowing unauthorised/inappropriate access to data can place a child or young adult at risk of physical harm.

3 Evaluate the Risks from the Privacy Impact and decide what should be done to Control the Risk

The first stage is to consider the risk associated with the privacy impact without any control measures in place. The matrix on the assessment form at Annex B helps quantify the risks.

L = Likelihood	S = Severity
5 = Almost Certain	5 = Severe
4 = Highly Likely	4 = Major
3 = Likely	3 = Serious
2 = Possible	2 = Moderate
1 = Unlikely	1 = Minor

The risk rating (R) is determined by multiplying the Likelihood with the Severity (R = L x S).

Low Risk = 1 – 7
Medium Risk = 8 – 15
High Risk = 16 - 25 (Do not proceed, consult with Professional Services Department)

Worked Example

Purchasing a subscription to an online software product – student email address is provided to the software company to create user accounts and students access and use the software online and their user activity is recorded. Demographic data, e.g. age, SEND status, Pupil Premium/other financial support is provided to create reports. The principal privacy impact is student personal information being passed to an external third party, and the data being stored outside the control of the TEN Group and security arrangements are unknown.

Risk rating with no controls**: Likelihood =3** (Likely) multiplied by **Severity = 3** (Serious) **R = 3 x 3 = 9 Medium Risk**.

The control measures to reduce the risk could be, assessing the third party for standards of security, putting a written and legally binding agreement in place, notifying students of the use, providing advice to students on keeping safe when online.

The residual risk rating could now be calculated as follows: **Likelihood = 1** (improbable) but the **Severity = 3** (Serious) does not change. The risk rating **with controls** would now be reduced to **(1 x 3) = 3** which is low risk.

When controlling risks a systematic approach should be used in deciding which control measures to implement, by considering the general hierarchy of control as follows:

- Elimination (Do we need to do this?).

- Substitution (Can the activity be replaced with another method/supplier?)
- Change the activity in order to reduce exposure to the risk. (e.g. limit the type of data provided if the Reports function is not required).
- Put in place specific legal requirements, e.g. written agreements with third parties, notices provided to data subjects)
- Practical controls (e.g. all data is anonymised).
- Issue instructions, advice or guidance to those involved.

Other control measures that may be appropriate are:

- Training.
- Written procedures.
- Monitoring and audit of the activity.

4 Record the Findings

It is important to record the findings on the risk assessment form **(Annex B)** to show that a proper check has been made and that there are suitable measures in place to control the risks. It is equally important that the person producing the risk assessment ensures that relevant staff and students are made aware of the assessments and that the control measures that are in place.

5 Review the Assessment and Update if Necessary

Risk assessments shall be reviewed annually to ensure that nothing has changed and that the control measures are effective. Triggers for review may also apply if:

- Significant change has occurred e.g. further data is to be collected/used.
- The supplier changes or is using a new sub-contractor
- An incident or near miss has occurred.

Annex A Low, Medium and High Risk Personal Data

Personal Data – Sensitive (Special Category) Information of identifiable individuals': - medical/health (incl. disability & related risk assessments/adjustments) - Race/Ethnicity - Religious & other similar beliefs - Sexual Life - TU membership - Biometric - Genetic- political affiliations/opinions - commission/allegations of unlawful act (incl. outcomes)	HIGH
Personal Data - Confidential Information of identifiable individuals which could cause substantial unwarranted damage or distress, e.g.: - set of identification details with the potential for fraud/identity theft (usually name, address, DOB, can include NI No, bank details, payroll no.) - images of children/young people (with or without names) - pastoral/HR records of conduct/behaviour, family circumstances, appraisal/performance record with personalised feedback/comment, allegations/investigations/outcomes of a disciplinary/performance nature, grievances	HIGH
Personal Data All other information of identifiable individuals, e.g: - student work, assessments, target/predicted grades, progression, grades/results - courses/study programmes undertaken/enrolled in and dates - employer sponsorship, funding, placements - career history, role profiles, attendance, salary/payroll/expenses, - next of kin/parent names & contact nos.	MEDIUM
Personal Data - work/study address information - work/student email address - work telephone number - work location & address - work job title	LOW

Annex B – Risk Assessment Form

TEN GROUP (CCN / CAN / WAN / WJAW / FAN / AAN / UTCN / Paston / NES)* ***delete as required***

RISK ASSESSMENT RECORD - WITH ALL CONTROL MEASURES IN PLACE

	Head of Department:	
	Assessor:	**Assessment Date:**

Activity/ Workplace Assessed:

Please provide full details of the activity (word picture) being undertaken.

HAZARD/ PRIVACY IMPACT	WHO might be affected?	PRECAUTIONS/CONTROLS already in place to remove hazard, reduce risk level	RISK (with controls)			✓ Additional Controls Needed.
			L	S	R	
	• **Students,** • **Staff,** • **Contractors,** • **Visitors,** • **Vulnerable persons,** • **Disabled persons,** • **Young persons.**	•				
	•	•				
	•	•				
	•	•				
	•	•				
	•	•				

Action Plan			
Additional Controls Needed	Action by	Target Date	Action Taken
Activities identified as requiring more specific assessments			

On completion your Head of Department is to approve this risk assessment and sign and date below.

Signed (Head of Department): Name:…… Signature:…… Date:……

The three columns (L,S,R) are for assessing the level or degree of risk. The first (L) is an assessment of the **likelihood** of the hazard/privacy impact taking place, the second (S) for the **severity** of the hazard/privacy impact, both based on the following:

RISK ASSESSMENT MATRIX

RISK						
Severity	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Likelihood				

LIKELIHOOD	
5	Almost Certain
4	Highly Likely
3	Likely
2	Possible
1	Unlikely

SEVERITY	
5	Severe
4	Major
3	Serious
2	Moderate
1	Minor

The third column (R) is for the level of risk which should be determined from inputting the L and S score into the risk matrix above.
The aim is to reduce the risk by prevention or control measures so far as is reasonably practicable.

Explanatory Note:

Risk

20-25	Do not proceed, consult the relevant NES Team
16-25	High (Do not proceed, consult the relevant NES Team)
8-15	Medium
1-7	Low

Severity

Severe	Multiple Fatality

Likelihood

Almost certain	Likely to occur
Highly Likely	More likely than not to occur
Likely	Has the potential to occur
Possible	Unlikely to occur There is a possibility that it could occur
Unlikely	Occurrence is extremely unlikely

	Group-wide regulatory or legal action with irrecoverable financial and reputational consequences
	Substantial and unwarranted damage or distress caused to multiple individuals
Major	Fatality
	Group-wide regulatory or legal action with substantial financial and reputational consequences
	Substantial and unwarranted damage or distress caused to an individual
Serious	Serious injury – reportable incident under RIDDOR such as fracture of bones, dislocation, amputation, occupational diseases (e.g. asthma, dermatitis), loss of sight
	Institution subject to regulatory enforcement action with moderate financial and reputational consequences
	Minor damage or distress caused to an individual
Moderate	Minor injury - First aid administered. Includes minor, cuts, bruising, abrasions and strains or sprains of ligaments, tendons, muscles
	Institution subject to complaint requiring internal inquiry
Minor	Near Miss – no injury, no data loss.