POLICY

Title: Data Protection

Policy Holder: Executive Manager

Approval Board: College Leadership Team

Version No: v3.2

Last reviewed: January 2026

Review period[1]: 2 Years

Summary: 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.

Accessibility: If you would like this information in an alternative format, e.g. Easy to Read, large print, Braille or audio tape, or if you would like the procedure explained to you in your language, please contact the College's marketing team on 01603 773 169.

Further information: If you have any queries about this policy or procedure, please contact the named policy holder or the College's marketing team on 01603 773 169.

Legislation or Regulation:	• UK General Data Protection Regulation • Data Protection Act 2018 • 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

Version Control Document			
Date	**Version No.**	**Reason for Change**	**Author**
Jan 2017	v 2.0	Rewrite / Incorporate 'current legislation'	D.Clarke
May 2017	v 2.3	Review	P.Beacock
Nov 2017	v 2.4	Contact number updated	P.Beacock
May 2018	v 2.5	Updated to reflect changes in legislation/regulation	P.Beacock
Aug 2019	v 2.6	Removal of UTCN References	P.Beacock
Jan 2021	v 2.7	Review	J.Mitchell
Mar 2021	v 2.8	Removal of TEN Group references	P.Beacock
Dec 2021	v 2.9	Removal of NES references	P.Beacock
Nov 2022 / Jan 2024	v 3.0	Review	Info Compliance
Feb 2025	V 3.1	Updates to sections 6.11 and 6.12. Text referencing out to CCTV Code of Practice and Records Management Policy	P.Beacock
Nov 2025 / Jan 2026	V3.2	Review	Info Compliance

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

Contents

1. Policy Statement

City College Norwich ("the College") is committed to maintaining high standards of data protection when processing personal data relating to employees, students, contractors, and visitors. The College will ensure compliance with all legal obligations under the UK General Data Protection Regulation (UK GDPR) and related legislation.

The CCN Board promotes a culture where the principles of UK GDPR and the Data Protection Act 2018 are understood and embedded in daily processes, with privacy considerations addressed early in planning activities.

2. Policy Aims & Objectives

This policy explains legislative requirements, sets expectations for compliance and directs staff to supporting procedures and guidance.

The College will:

- Process personal data fairly, lawfully, and for specified purposes, recording activities in an information asset register.
- Assign clear responsibilities for data protection compliance.
- Conduct privacy impact assessments for new or changed processing.
- Maintain a compliance system with regular audits, inspections, and action reviews.
- Put Data Sharing Agreements in place for regular data sharing.
- Complete checks and implement Data Processor Agreements for third-party processors.
- Provide clear notifications and privacy notices to staff, students, and parents on personal data processing.
- Respond appropriately to individuals exercising their rights under legislation.
- Deliver training and guidance for staff handling personal data.
- Record, investigate, and report personal data incidents or breaches where required.
- Allocate resources to ensure secure processing across all College sites and workplaces.
- Maintain records that document what data the College holds, shares and processes.

3. Definitions

Personal Data: Information that identifies a living individual, either directly (e.g., name) or indirectly when combined with other data. It includes:

- Data stored electronically or in structured manual records (e.g., education, staff or health records).
- Opinions or intentions about a person.
- Pseudonymised data (e.g., key-coded), if re-identification is possible.

Special Category Data: Data requiring extra protection under UK GDPR, including:

- Racial or ethnic origin
- Biometric or genetic data, (where used for identification purposes)
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health information
- Sex life or sexual orientation

Processing: Any activity involving personal data, such as collecting, storing, transferring, amending, or deleting.

Data Subject: The individual to whom the data relates.

Data Protection Officer (DPO): Oversees policy implementation, monitors compliance, develops guidance, and acts as the main contact for individuals and the ICO.

Data Controller: Determines the purpose and manner of processing personal data (usually the organisation or governing body).

Data Processor: Processes personal data on behalf of the Data Controller (not an employee).

Third Party: Any person or organisation outside the College, its trustees, employees, and data subjects.

4. Scope

This policy applies to all personal data created, received, maintained, or processed by College staff in the course of their duties. It also covers personal data handled by external parties or contractors on behalf of the College.

5. Legal Requirements

UK GDPR / Data Protection Act 2018: The UK GDPR and DPA 2018 are the main laws governing personal data. They require compliance with the principles in Article 5 of UK GDPR:

- Process data lawfully, fairly, and transparently
- Collect for specified, legitimate purposes
- Ensure data is adequate, relevant, and limited to what's necessary
- Keep data accurate and up to date
- Retain data only as long as needed
- Protect data with appropriate security measures

Post-Brexit, UK GDPR remains in domestic law alongside an amended DPA 2018, with scope for future review.

Other relevant legislation includes:

- Privacy and Electronic Communications Regulations 2003 – direct marketing and electronic communications
- Computer Misuse Act 1990 – unauthorised access/modification
- Freedom of Information Act 2000 – access to public authority information
- Protection of Freedoms Act 2012 – biometric data requirements
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) Regulations 2000

Education specific legislation also impacts personal data processing (see Appendix 1).

6. Procedure

6.1 Monitoring the Implementation and Effectiveness of the Policy

The Information Compliance team, monitors this policy through audits, incident reports, and statistics on data breaches, DPIAs, and information requests. Information Compliance also report to the Data Controllers and recommends actions where necessary.

6.2 Registration with the ICO and the Data Protection Fee

The College is registered with the Information Commissioner's Office for personal data processing, with renewals managed by the Information Compliance team. Any changes to processing activities must be reported to the team so the registration can be updated.

6.3 Privacy by Design / Privacy by default

The College demonstrates data protection is embedded in all processing activities by:

- Appointing a qualified DPO with resources to maintain expertise.
- Processing only necessary personal data in line with UK GDPR principles.
- Completing DPIAs for high-risk processing or new technologies (with DPO advice).
- Designing IT systems, services, and processes with privacy in mind.
- Embedding privacy in organisational policies, practices, and strategies.
- Providing regular staff training on data protection and related policies.
- Conducting audits and reviews to ensure compliance.
- Maintaining records of processing activities, including:
  - Public information via privacy notices (DPO contact details and data use).
  - Internal records detailing data types, purposes, recipients, storage, retention, and security measures.

6.4 Data Protection Impact Assessments

DPIAs are a UK GDPR requirement and must be integrated into planning for any new project or activity involving personal data that poses a high risk to individuals, such as new technologies or off-site processing.

Privacy risks should be assessed early, with measures and controls documented. The Project Leader or Manager completes the DPIA in consultation with stakeholders and the Information Compliance team. A member of the Group LeadershipTeam (GLT) will sign off the DPIA, and where residual risk remains; endorses organisational acceptance of risk. Where high risk remains, the DPIA can be escalated to an executive lead (member of ELT) via the Director of Legal & Governance. DPIA forms and guidance are available internally via the Communications tab

6.5 Staff Training and Awareness

All new staff receive data protection training during induction.

Mandatory Data Protection Core Training must be completed by all staff via an online module and repeated every two years. The Principal and Managers ensure completion, while the Training and Development team monitors compliance and reports regularly to the Information Compliance team.

Staff failing the end of course test twice are referred for additional training; persistent failure may lead to performance or disciplinary action.

Additional or bespoke training is available on request or as identified through DPIAs, audits, or development needs. Guidance and support materials are provided internally with alternative formats available.

6.6 Audit

The Information Compliance Team audits the College's compliance with legislation and this policy. After each audit, an improvement action plan is developed and agreed with the College.

6.7 Privacy Notices and Communication to Data Subjects

The UK GDPR (Articles 12-15 and 22 and 34), obligates the College to inform data subjects how their personal data is processed. The Information Compliance team produces privacy notices, published on College websites and issued with admissions forms or at other data collection points, such as staff recruitment.

A privacy notice includes:

- Details of the Data Controller
- Purposes for processing
- Data sharing arrangements
- Data subject rights

New data collection or processing arrangements may require updated notices. Managers must ensure all forms and technologies used to gather personal data include a privacy notice at the point of collection.

Staff related privacy notices are available internally, under the Communications tab.

Notices should be clear and appropriate for the audience, 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')

Personal data must be processed for a legitimate educational purpose, align with the College's governing documents, and meet conditions under UK GDPR Articles 6 (and 9 and10 where applicable).

Consent

Consent is required only when no other lawful basis applies. It must be freely given and easily withdrawn without detriment. Under UK GDPR, consent grants additional rights, including data deletion when withdrawn. For online services offered to students, parental consent may be required (except for counselling or preventive services).

Right to Erasure ('Right to be Forgotten')

Under Article 17, individuals can request deletion of personal data in certain circumstances, such as:

- Data no longer needed for its original purpose
- Consent withdrawn
- Legitimate interest challenged with no overriding reason
- Direct marketing objections
- Unlawful processing
- Legal obligation
- Processed the personal data to offer information society services to a child.

Enhanced protection applies to children's data, especially online.

6.9 Limitation, minimisation and accuracy

The College collects personal data only for specified, legitimate purposes, explained at the point of collection.

If data is used for a new purpose, individuals will be informed and consent obtained where required.

Staff must process personal data only when necessary for their role and delete or anonymise it when no longer needed, in line with the College's records management retention schedule.

6.10 Use of Personal Images, Photographs and Videos

Images can identify individuals and may reveal sensitive data (e.g., ethnicity or disability). The College also holds other information (such as names) that can link to images for further identification.

The taking, use, and sharing of personal images must comply with UK GDPR Article 5, like any other personal data. Students, staff, and others must be informed when and why images are taken, and consent obtained if the purpose is unrelated to education or not covered by the College's privacy notice.

The College does not impose a blanket ban on parents/carers taking photos for personal use at events. Restrictions should only apply in exceptional safeguarding cases and must be communicated in advance. Decisions may vary depending on the event and students involved.

Further guidance, including best practice for handling images, is available in the Use of Personal Images Guidance Note under the Communications tab.

6.11 Closed Circuit Television (CCTV)

CCTV is used to enhance safety and security, deter crime, and assist in investigations. While effective, CCTV is intrusive and must be properly assessed, implemented, and monitored in line with legislation and codes of practice.

College CCTV is used for:

- Crime prevention and detection
- Responding to inappropriate behaviour, harassment, or public order issues
- Supporting security patrols and reducing fear of crime
- Creating a safer community and gathering evidence fairly
- Assisting emergency services
- Meeting CITB exam compliance requirements
- Investigating exam malpractice or complaints
- Supporting internal investigations and disciplinary hearings
- Ensuring safety of campus users and property
- Farm management and livestock monitoring at Easton campus
- Establishing, exercising, or defending legal rights

Siting CCTV Cameras in areas where it could be construed that they are being used to monitor or measure employee performance should be avoided.

Any changes to CCTV use must be reported to the Information Compliance team for data protection updates.

Requirements for CCTV use:

- DPIA completed for new or changed use
- Privacy Notice published stating CCTV use and purpose
- Designated staff appointed as CCTV Operators
- Consultation with Information Compliance team and adherence to the CCTV Code of Practice

Further details are available in the **CCTV Code of Practice** under the Communications tab.

6.12 Personal Data and Social Media

Sharing personal data on social media (e.g., X (Formally Twitter), Facebook) places it in the public domain, where it can be widely redistributed. Staff must ensure any such use complies with UK GDPR and refer to the College's Social Media Policy for guidance.

6.13 Data Sharing Agreements

When personal data is regularly exchanged between organisations and both make decisions about its use, a Data Sharing Agreement (DSA) is negotiated. The DSA sets out:

- Legal basis and purpose for sharing
- Data description
- Responsibilities for UK GDPR compliance
- Security measures
- Termination process

Managers must consult the Information Compliance team before starting or changing any regular data-sharing arrangement to ensure agreements are documented, risks assessed, and privacy notices updated.

Further guidance is available in the Personal Data Disclosure Guidance Note under the Communications tab.

6.15 Third Party Requests for Disclosure of Personal Data

When a third-party processes personal data for the College, the Information Compliance team reviews their data protection arrangements and, where appropriate, negotiates a Data Processor Agreement (DPA). The DPA ensures:

- Processing follows College instructions and UK GDPR
- Adequate security measures protect against loss, damage, or unauthorised access
- Personnel with access are reliable
- Clear procedures for SARs, complaints, and breaches
- Proper termination and data disposal arrangements

DPIAs identify the need for a DPA early in planning. Directors and Managers must consult the Information Compliance team before engaging any third-party processor. Further guidance is in the Personal Data Disclosure Guidance Note under the Communications tab.

Where there is a regular and routine need to share information between organisations, a Data Sharing Agreement is needed. (See item 6.13)

6.16 Subject Access Requests

All individuals (staff, students, and other data subjects) have the right to access personal data held about them. Requests can be made verbally or in writing but must clearly state what data is being requested.

The Information Compliance team handles all Subject Access Requests for the College and ensures they are processed promptly, within one calendar month.

6.17 Professional Content

Personal data includes opinions and intentions about individuals, recorded in any format (e.g., notes, emails, MS Teams Chat, note books, personal files, interview notes). All information about individuals must be professional in tone, accurate where possible, and based on reliable sources.

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

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A breach of UK GDPR occurs when personal data is not processed in line with Article 5 and may involve loss, theft, damage, or unauthorised disclosure. Breaches often impact individuals' privacy and can cause financial or other harm.

Complaints about data handling can be made by anyone whose data the College holds and will be managed under the Complaints Policy with advice from the Information Compliance team. Staff concerns can be raised with their Line Manager, the College Data Protection Officer or Information Compliance team,

Staff must report suspected breaches or complaints to their Line Manager. Managers must notify the Information Compliance team and complete a Personal Data Incident Report. The team will investigate, recommend actions, and determine if a legal breach occurred. Certain breaches must be reported to the ICO within 72 hours, in consultation with the Principal/Governing Body.

Where staff actions cause a breach, disciplinary or performance management processes may apply. Intentional or negligent disregard of policy may lead to a finding of gross misconduct or criminal proceedings may be necessary.

Further guidance and templates are available in the Personal Data Incident Management Guidance Note under the Communications tab.

6.19 Records Management

All records, including those containing personal data, are subject to the Records Management Policy and Retention Schedule (available under the Communications tab). Records must be stored and logged so they can be located for business needs and legal requirements, such as Subject Access or Freedom of Information requests.

The College is responsible for secure, accessible local storage and timely disposal of records. The Information Compliance team oversees off-site commercial storage.

6.20 Secure Storage and Handling of Personal Data

All staff receive training and guidance on security measures for handling personal data, including:

- Secure storage
- Locking screens when unattended and using screen filters
- Permission-based electronic storage
- Secure sharing via encrypted networks and approved cloud services
- Use of College-issued encrypted mobile devices.
- Use of personal devices (Working from home) etc.

For more details, refer to the Information Security Policy and Records Management Policy, held on the Communications tab, or contact IT Services or the Information Compliance Team.

6.21 Disposal of Personal Data

Hard Copy Records: Dispose of personal data in paper form as confidential waste using designated bins/sacks, following the Disposal of Confidential Waste Guidance Note and local procedures.

Digital Records: Treat electronic data with the same care as paper records. While IT Services assist with disposal, this does not cover all areas (e.g., departmental SharePoint sites). Staff are responsible for managing and deleting digital files when no longer needed.

Hardware: IT Services handle the disposal of devices containing personal data in line with the Information Security Policy.

The disposal of personal data, in any format, must be carried out in accordance with the College's Records Management Policy and Retention Schedule

6.22 Room and Building Re-assignments

Moving work locations can lead to personal data being mishandled, lost, left behind or disposed of incorrectly. Managers and staff must ensure that any hard copy personal data in rooms being vacated is managed securely by:

- Transporting personal data in sealed, labelled boxes with the owner and destination.
- Conducting a full sweep of the vacated room, including cupboards and cabinets.
- Disposing of any personal information securely (see 6.21).

Each college campus may set local procedures to manage moves appropriately.

6.23 Staff Leavers/Transfers to new role

When a staff member leaves or moves to a new role, their Line Manager must ensure all personal data, both hard copy and digital, is properly managed. This means the data should be reassigned to a new responsible person, stored in an appropriate shared area, or archived or securely destroyed as required.

For staff leaving the College, HR Services will initiate the Staff Leaver procedure. Staff must not retain or copy any College personal data and are required to return ID cards, keys, access cards, and any issued IT equipment.

Managers should ensure access to systems, databases, shared storage areas, and physical locations is revoked and reset when staff change roles or leave the College.

6.24 Use of Email

Email is vulnerable to data breaches, such as sending personal data to the wrong recipient, using non-secure connections, or including inappropriate information in email chains.

Depending on the sensitivity of the data, protective measures should be used, such as anonymising details, password-protecting attachments, or applying encryption.

Further guidance is available in the Handling Email Guidance Note under the Communications tab.

6.25 Use of Office 365 (O365)

Office 365 provides secure options for storing and sharing data. Instead of sending attachments by email, staff should consider sharing documents via secure links in SharePoint or OneDrive. Sharing data external to the college may be restricted on some college Sharepoint sites. This approach supports collaboration, reduces multiple versions, and allows better control over access and audit trails.

Although O365 offers strong protection, additional measures, such as those used for email, may still be necessary depending on the sensitivity of the data.

Further guidance is available in the Handling Email Guidance Note under the Communications tab on the College homepage.

6.26 Use of Fax

Fax is vulnerable to data breaches due to risks such as incorrect numbers and uncertainty about the receiving machine's location, which may be in shared or open areas.

As a rule, fax should not be used for personal information. If absolutely necessary for urgent cases where email encryption is unavailable, steps must be taken to reduce risk: confirm the fax number with the recipient, double-check the number entered, ensure the recipient is at the machine during transmission, and confirm receipt in full.

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

Before buying equipment or software for storing or processing personal data, such as mobile devices, surveillance tools, or cloud services, the College must assess privacy risks and consult IT Services and the Information Compliance team. Advice should cover security, encryption, and product suitability. All systems and software must follow the principle of privacy by design to meet UK GDPR requirements.

6.28 Marketing

Under UK GDPR, individuals have the right to prevent their personal data from being used for direct marketing. Managers must ensure all marketing activities comply with UK GDPR and the Privacy & Electronic Communications Regulations 2003.

The Information Compliance Team can advise on ensuring marketing is covered by the privacy notice and ICO registration, updating where necessary. Individuals should be notified when the college intends on using their data to market to them, giving them the option to refuse consent.

6.29 Contractors & Visitors

Contractor conduct, including confidentiality and compliance with data protection law, is covered in the Site Rules. Contractors and visitors must report any unauthorised access to personal data during their visit, for example, unlocked screens or documents left out, by notifying Estates and Facilities.

Contractors and visitors are responsible for any personal data they bring onto College premises.

7. Organisational Responsibilities

7.1 Governing Body / Principal & Senior Management

The governing body acts as the College's Data Controller, with overall accountability for ensuring personal data is processed fairly, lawfully, and securely. This includes setting the strategic direction, providing oversight, and ensuring compliance with the Data Protection Policy.

Responsibility is delegated to the CEO and Principal, the Senior Management Team (SMT) and Group Leadership Team.

The Data Controller must ensure adequate resources are in place to meet statutory requirements, including appropriate technical and organisational measures, staff training, and effective implementation of data protection arrangements.

7.2 All Staff

All staff must:

- process personal data fairly, lawfully, and securely
- seek guidance if data may be at risk of damage, loss, or unauthorised disclosure
- report any UK GDPR incidents or breaches
- comply with all data protection requirements
- maintain data protection knowledge through mandatory training

Regardless of whether they handle personal data directly, all staff are required to follow UK GDPR principles and requirements.

7.3 The Information Compliance team

The Information Compliance team coordinates data protection matters, focusing on guidance and advice for Data Controllers on legislation requirements and application. The Data Protection Officer (DPO), leads policy development, strategic planning, and alongside the Director of IT Services, data security across the College.

Key responsibilities of the DPO:

- Oversee implementation of data protection legislation
- Provide competent advice to managers and staff
- Report on data protection performance
- Promote and identify compliance training for all staff
- Foster a culture of privacy and compliance
- Monitor and audit data protection practices
- Explore shared compliance services with external organisations

7.4 Director of IT Services

The Director of IT Services is responsible for managing security measures to protect personal data in all formats including electronic, images, and paper.

Key responsibilities:

- Ensure appropriate technical measures protect electronic personal data and advise on physical security for other formats
- Work with the Information Compliance team to align security advice and training content
- Notify the Information Compliance team of projects, procurement, or process changes involving personal data, and assist with Data Protection Impact Assessments (DPIAs)

8. Reference to other relevant policies and procedures

- Information Security Policy
- Records Management Policy
- Social Media Policy
- Freedom of Information Policy

- Student / Staff IT Acceptable Use Policy

- Records Retention Schedule
- Disclosure of Personal Information Guidance Note
- Handling Email Guidance Note
- Use of Personal Images Guidance Note
- Disposal of Confidential Waste Guidance note
- CCTV Code of Practice

9. Contact

For more information about this policy, contact the Information Compliance Team:
Telephone: 01603 773585 / 3176
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 an EU law on data protection and privacy for individuals in the EU and EEA. It also governs the transfer of personal data outside these areas. Its main purpose is to give individuals control over their personal data and create a unified regulatory framework for businesses.

The GDPR sets legal requirements for processing personal data and includes sanctions for breaches, including criminal offences for unauthorised disclosure.

Following Brexit, the GDPR remains in UK law as the UK GDPR, alongside an amended Data Protection Act 2018, with scope for future review.

Data Protection Act 2018 (DPA 2018)
The Data Protection Act 2018, which received Royal Assent on 23 May 2018, modernises UK data protection law for the digital age. It applies the EU GDPR standards while setting out UK-specific provisions as national law.

Privacy & Electronic Communications (EC Directive) Regulations 2003
These regulations make it unlawful to send direct marketing without prior consent, unless there is an existing relationship between the parties.

Note: Amendments were made in 2004, 2011, and 2016.

Freedom of Information Act 2000 (FOI)
This Act requires public bodies to manage records so information is retained only as long as necessary and remains identifiable and retrievable. It also gives anyone the right to request information held by a public authority.

Note: The Act applies only to certain parts of the College—see the FOI Policy for details.

Protection of Freedoms Act 2012
This Act requires:
- Parental consent for schools and colleges to collect biometric data
- Regulation of CCTV use for surveillance

Computer Misuse Act 1990
This Act protects computer systems from unauthorised access or modification. Hacking and introducing viruses are criminal offences under this law.

Investigatory Powers Act 2016
This Act sets limits on covert surveillance, including phone tapping, interception of correspondence, and covert filming (e.g., CCTV). Intercepting private communications is unlawful unless carried out under the provisions of the Act.

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
This legislation allows businesses to intercept communications on their own networks for legitimate purposes, such as detecting email or internet misuse and recording calls to evidence transactions.

Education Specific Legislation and Statutory Guidance
Various laws and guidance provide explicit or implied powers to collect, use, and share personal data (this list is not exhaustive):

- Children Act (various dates)
- Education Act (various dates)
- Education & Skills Act
- Department for Education Statutory Guidance