Caedmon College Whitby

Data Protection and Information Policy

College Governance Status

This policy was re-issued in June 2014 and was adopted by the Governing Body on 26 June 2014 and updated in June 2016. It will be reviewed annually or in light of any new guidance or legislation, as required.

Review dates	By Whom	Approval dates
October 2020	Staff and Governors	December 2020
October 2021	Staff and Governors	October 2021
November 2022	Staff and Governors	November 2022

Signed by the Chair:

S Crossland

C Zanelli

DATA PROTECTION AND INFORMATION POLICY

Introduction

This policy is to ensure that Caedmon College Whitby complies with the requirements of the General Data Protection Regulation, Environmental Information Regulations 2004 (EIR) and Freedom of Information Act 2000 (FOIA), associated guidance and Codes of Practice issued under the legislation.

Scope

The Information Policy applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

Information Security and security incident reporting will be addressed in separate policies.

Data Protection

Personal data will be processed in accordance with the requirements of GDPR and in compliance with the data protection principles specified in the legislation.

The school has notified the Information Commissioner's Office that it is a Data Controller and has appointed a Data Protection Officer (DPO). Details of the DPO can be found here:

Information Governance
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL
schoolsDPO@veritau.co.uk
01609 53 2526

The DPO is a statutory position and will operate in an advisory capacity. Duties will include:

- Acting as the point of contact for the Information Commissioner's Office (ICO) and data subjects;
- Facilitating a periodic review of the corporate information asset register and information governance policies;
- Assisting with the reporting and investigation of information security breaches
- Providing advice on all aspects of data protection as required, including information requests, information sharing and Data Protection Impact Assessments; and
- Reporting to governors on the above matters

Information Asset Register

The DPO will advise the school in developing and maintaining an Information Asset Register (IAR). The register will include the following information for each asset:

- An individual information asset identification number;
- The owner of that asset;
- Description and purpose of the asset;
- Whether there is a privacy notice published for that asset;
- Format and location of the asset;
- Which officers (job titles/teams) have routine access to the information;
- Whether there are any data sharing agreements relating to the information and the name of that agreement,
- Conditions of data processing;
- Details of any third parties contracted to process the information;
- Retention period for the asset

The IAR will be reviewed annually and the Head Teacher will inform the DPO of any significant changes to their information assets as soon as possible.

Information Asset Owners

An Information Asset Owner (IAO) is the individual responsible for an information asset, understands the value of that information and the potential risks associated with it. The school will ensure that IAO's are appointed based on sufficient seniority and level of responsibility.

IAO's are responsible for the security and maintenance of their information assets. This includes ensuring that other members of staff are using the information safely and responsibly. The role also includes determining the retention period for the asset, and when destroyed, ensuring this is done so securely.

Training

The school will ensure that appropriate guidance and training is given to the relevant staff, governors and other authorised school users on access to information procedures, records management and data breach procedures. Individuals will also be made aware and given training in relation to information security including using email and the internet.

The DPO will be consulted in relation to training where necessary; to ensure training resources and their implementation are effective.

The school will ensure that any third party contractors have adequately trained their staff in information governance by carrying out the appropriate due diligence.

Privacy notices

Caedmon College Whitby will provide a privacy notice to data subjects each time it obtains personal information from or about that data subject. Our main privacy notice will be displayed on the school's website in an easily accessible area. This notice will also be provided in a hard copy to pupils and parents at the start of the year as part of their information pack. A privacy notice for employees will be provided at commencement of their employment with the school. Specific privacy notices will be issued where the data subject requires more information about specific processing (e.g. school trips, projects).

Privacy notices will be cleared by the DPO prior to being published or issued. A record of privacy notices shall be kept on the school's Information Asset Register.

Information sharing

In order to efficiently fulfil our duty of education provision it is sometimes necessary for the school to share information with third parties. Routine and regular information sharing arrangements will be documented in our main privacy notice (as above). Any adhoc sharing of information will be done in compliance with our legislative requirements.

Data Protection Impact Assessments (DPIAs)

The school will conduct a data protection impact assessment for all new projects involving high risk data processing as defined by GDPR. This assessment will consider the privacy risks and implications of new projects as well as providing solutions to the identified risks

The DPO will be consulted at the start of a project and will advise whether a DPIA is required. If it is agreed that a DPIA will be necessary, then the DPO will assist with the completion of the assessment, providing relevant advice.

Retention periods

Retention periods will be determined by any legal requirement, best practice or national guidance, and lastly the organisational necessity to retain the information. In addition IAOs will take into account the Limitation Act 1980, which provides timescales within which action may be taken for breaches of the law, when determining retention periods.

Destruction of records

Retention periods for records are recorded in the school's IAR. When a record reaches the end of its retention period the IAO will arrange for the records, both electronic and paper to be destroyed securely. Provisions to destroy paper information securely include cross cutting shredders and confidential waste bins. Advice in regards to the secure destruction of electronic media will be sought from relevant IT support.

A record should be retained of all files destroyed including, where relevant:

- File reference number,
- Description of file,
- Date of disposal,
- Method of disposal,
- Officer who destroyed record

Third party Data Processors

All third party contractors who process data on behalf of the school must be able to provide assurances that they have adequate data protection controls in place to ensure that the data they process is afforded the appropriate safeguards. Where personal data is being processed, there will be a written contract in place with the necessary data protection clauses contained. Relevant senior leadership may insist that any data processing by a third party, ceases immediately if it believes that that third party has not got adequate data protection safeguards in place. . If any data processing is going to take place outside of the EEA then the Data Protection Officer must be consulted prior to any contracts being agreed.

Access to information

Requests for information under the Freedom of Information Act 2000 and Environmental Information Regulations 2004

Requests under this legislation should be made to officejobs@ccwhitby.org

FAO Katie Mallender to:

- Deciding whether the requested information is held;
- Locating, retrieving or extracting the information;
- Considering whether any exemption might apply, and the balance of the public interest test;
- Preparing the material for disclosure and drafting the response;
- Seeking any necessary approval for the response; and
- Sending the response to the requester

  FOIA requests should be made in writing. Please note that we will only consider requests which provide a valid name and address and we will not consider requests which ask us

to click on electronic links. EIR requests can be made verbally, however we will endeavour to follow this up in writing with the requestor to ensure accuracy.
Each request received will be acknowledged within 5 school days. The Chair of Governors and Head Teacher will jointly consider all requests where a public interest test is applied or where there is any doubt on whether an exemption should be applied. In applying the public interest test they will:

- Document clearly the benefits of both disclosing or withholding the requested information; and
- Where necessary seek guidance from previous case law in deciding where the balance lies
- Consult the DPO

Reasons for disclosing or not disclosing will be reported to the next governing body meeting.
We have adopted the Information Commissioner's model publication scheme for schools and will publish as much information as possible on our website in the interests of transparency and accountability.
We will charge for supplying information at our discretion, in line with current regulations. If a charge applies, written notice will be given to the applicant and payment must be received before the information is supplied. We will follow NYCC charging policy for FOI/EIR. We will adhere to the required FOI/EIR timescales, and requests will be answered within 20 **school days.**

Requests for information under the GDPR- Subject Access Requests
Requests under this legislation should be made to post@ccwhitby.org
Any member of staff/governor/trustee may receive a request for an individual's personal information. Whilst GDPR does not require such requests to be made in writing, applicants are encouraged where possible to do so; applicants who require assistance should seek help from the school. Requests will be logged with the administration team and acknowledged within 5 days.

We must be satisfied as to your identity and may have to ask for additional information such as:

- Valid Photo ID (driver's licence, passport etc);
- Proof of Address (Utility bill, council tax letter etc);
- further information for the school to be satisfied of the applicant's identity;

Only once the school is satisfied of the requestor's identity and has sufficient information on which to respond to the request will it be considered valid. We will then respond to your request within the statutory timescale of 30 **calendar** days.

The school can apply a discretionary extension of up to 60 calendar days to comply with the request if the requested information would take a considerable amount of time to collate, redact, and prepare for disclosure due to either the complexity or voluminous nature of the records. If we wish to apply an extension we will firstly seek guidance from our DPO, then inform the applicant of the extension within the first 30 days of receiving the request. This extension period will be kept to a minimum and will not be used as a way of managing workloads. In very limited cases we may also refuse a request outright as 'manifestly unreasonable' if we would have to spend an unjustified amount of time and resources to comply.

Should we think any exemptions are necessary to apply we will seek guidance from our DPO to discuss their application.

If a subject access request is made by a parent whose child is 12 years of age or over we may consult with the child or ask that they submit the request on their own behalf. This decision will be made based on the capacity and maturity of the pupil in question.

Requests received from parents asking for information held within the pupil's Education Record will be dealt with under the Education (Pupil Information)(England) Regulations 2005. Any charges which arise from this request will be applied at our discretion.

Data Subject rights

As well as a right of access to information, data subjects have a series of other rights prescribed by the GDPR including:

- Right to rectification
- Right to erasure
- Right to restrict processing
- Rights in relation automated decision making and profiling

All requests exercising these rights must be in writing and forwarded to Kate Mallender who will acknowledge the request and respond within 30 calendar days. Advice regarding such requests will be sought from our DPO.

A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

Complaints

Complaints in relation to FOI/EIR and Subject Access will be handled through our existing procedures. Any individual who wishes to make a complaint about the way we have handled their personal data should contact the DPO on the address provided.

Copyright

Caedmon College Whitby will take reasonable steps to inform enquirers if any third party might have a copyright or intellectual property interest in information provided in response to their requests. However it will be the enquirer's responsibility to ensure that any information provided by the school is not re-used in a way which infringes those interests, whether or not any such warning has been given.

MAKING INFORMATION AVAILABLE

The College, as a public body, is open and accountable and will make information available in line with the Data Protection Act, Environmental Regulations and Freedom of Information Act and will only apply exemptions when absolutely necessary. If an exemption applies individuals will be advised they cannot have the information they have requested and, and where appropriate, given the reason why information is being withheld.

The College will make all information that it holds available unless an exemption is applied or, in respect of FOIA, the cost of supplying the information exceeds the regulatory cost threshold (currently £450), or the enquirer, having been notified of the charges applicable, does not pay.

- The College already makes most reports, minutes and reasons for decisions available to the public on request, which complies with the spirit of the legislation to promote openness and accountability.

Personal Data will be collected, stored, used and disclosed with due regard to the requirements of the Data Protection principles. Requests for personal data will be dealt with under the terms of the Act. Requests for environmental information will be dealt with in accordance with Environmental Information Regulations. All other request for information will be dealt with under the terms of the Freedom of Information Act. Relevant staff will be provided with training on access to information regimes as required.

Subject Access Requests will be dealt with following the GDPR regulations – within one month, and will be free of charge.

A Publication Scheme will be maintained, in line with the FOIA, and will list the information the College makes readily available, it will advise how it can be obtained and whether any charges apply. The Publication Scheme will be updated as and when appropriate and will be subject to review by the Governing Body.

Responsibility

The Chair of Governors and the Principle will jointly consider all requests where a public interest test is applied, or where there is any doubt on whether or not an exemption should be applied. In applying the public interest test they will:

- Document clearly the benefits from both disclosing and withholding the requested information; and
- Where necessary seek guidance on case law in deciding where the balance lies. Reasons for disclosing/not disclosing the information will be reported to the next governing body meeting.

  The day-to-day responsibility for implementation of the College's governing body's Information Policy and the provision of advice, guidance, publicity and interpretation of the policy is delegated to the Principal.

The Principal will:

- oversee all requests for information
- ensure systems are in place to deal with requests and to co-ordinate/update the Publication Scheme
- consider what information, training and guidance staff may need
- be responsible for maintaining a log of all request received and for ensuring they are responded to within the prescribed timescales
- ensure a record of refusals and reasons for refusals is kept, allowing the governing body to review the College Information Policy on an annual basis
- take a view on possibly sensitive areas.

How the College manage requests for information

- The College will provide reasonable advice and assistance to individuals if they need help in putting a request for information together;
- Requests will be acknowledged within one school day.
- If there is any doubt on the scope of information requested clarification will be sought from the applicant.
- Requests will be responded to within the prescribed timescales.
- In some cases the disclosure of information may affect the rights of a third party. In such circumstances the College will ensure that disclosure of such information will be in line with FOI, DP and EIR legislation.
- Where the College receives a request to be dealt with under FOIA and some or all of the information is not held by the College and it is believed that another public authority may hold that information, then the College will ask the applicant if they wish the request to be transferred to the other authority once the information, held by the College has been disclosed. If the College is unable to facilitate the transfer of the request for information to another authority then, where possible, the applicant will be offered advice to enable him/her to pursue the request.
- The College will comply with its obligations on requests transferred by another public body in the same manner it would had the request been received directly by the College.

- Data sent by email will be encrypted and the password will be given by a means other than email.

Charging for providing information

Charging for supplying information will be at the College's discretion and in line with current regulations. If a charge applies, written notice will be given to the applicant and payment must be received before the requested information is supplied.

- **FOI & EIR** requests the College will use the North Yorkshire County Council Charging Policy (a copy of which can be located in the NYCC Schools Information Governance Manual Section B, Appendix 4). Once the individual has been notified that a fee is payable, if this is not received within 3 months of the notification, the request will be deemed to have lapsed.

- **DP** - charges will be made in line with current regulations.

If a charge applies, written notice will be given to the applicant and this should be promptly paid, usually prior to receiving the information.

Monitoring & Evaluation

The Principal will be responsible for periodically monitoring requests received and action taken to ensure that the College is complying with it information legislation and report annually to the Governing Body.

Complaints

Expressions of dissatisfaction will be handled through the College's existing general complaints procedure.

RECORDS MANAGEMENT/SECURITY & CONTROL OF INFORMATION

The College recognises that the efficient management of its records and information is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the College.

- The College will ensure that records are managed in line with the NYCC guidance.
- Protocols will be in place to ensure the College knows what information is held and by whom.
- The College will use the North Yorkshire County Council (NYCC) Schools' Record Retention and Destruction Schedule (RRDS) and will ensure records are retained for the appropriate period and no longer, unless there are special reasons for doing so. (A copy of the NYCC RRDS can be located in the NYCC Schools' Information Governance Manual Section B, Appendix 3).
- The College will ensure that records are held safely and securely. With access restricted where appropriate.
- The College will ensure that use of email is properly controlled in line with NYCC guidance.
- The College will ensure that use of the Internet is properly controlled in line with NYCC guidance.

HANDLING OF DISCLOSURE INFORMATION

General principles

As an organisation using the Criminal Records Bureau (CRB) service to help assess the suitability of applicants for positions of trust, Caedmon College Whitby complies fully with the CRB Code of Practice regarding the correct handling, use, storage, retention and disposal

of Certificates and Certificate information. It also complies fully with its obligations under the Data Protection Act 1998 and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of Certificate information and has a written policy on these matters, which is available to those who wish to see it on request.

Storage and access

Certificate information should be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

Handling

In accordance with section 124 of the Police Act 1997, Certificate information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom Certificates or Certificate information has been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it.

Usage

Certificate information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Retention

Once a recruitment (or other relevant) decision has been made, we do not keep Certificate information for any longer than is necessary. This is generally for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints. If, in very exceptional circumstances, it is considered necessary to keep Certificate information for longer than six months, we will consult the CRB about this and will give full consideration to the Data Protection and Human Rights of the individual before doing so. Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.

Disposal

Once the retention period has elapsed, we will ensure that any Certificate information is immediately destroyed by secure means – ie, by shredding, pulping or burning. While awaiting destruction, Certificate information will not be kept in any insecure receptacle (eg, waste bin or confidential waste sack). We will not keep any photocopy or other image of the Certificate or any copy or representation of the contents of a Certificate. However, notwithstanding the above, we may keep a record of the date of issue of a Certificate, the name of the subject, the type of Certificate requested, the position for which the Certificate was requested, the unique reference number of the Certificate and the details of the recruitment decision taken.

TRAINING

The College will ensure that appropriate guidance and training is given to the relevant staff, governors and other authorised College users on handling requests, records management, security and access to information, using Emails and the Internet.

COPYRIGHT

When providing information, the College will ensure that there is no infringement of copyright legislation.

GENERAL

Any user who contravenes this guidance will be dealt with appropriately. This may include disciplinary action and/or informing the Police where appropriate.

Information Security

The objectives of this section of the policy are to help the College to preserve:

- Confidentiality - access to data shall be confined to those with appropriate authority.

- Integrity – information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specifications and legislation.

- Availability - Information shall be available and delivered to the right person, at the time when it is needed and in the relevant format.

The College aims to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the College by:

- ensuring that all employees and members are aware of and fully comply with the relevant legislation, as described in this and other policies

- describing the principles of security and explaining how they shall be implemented in the College

- information includes data printed out or written on paper, stored on computers, transmitted across networks, sent by fax, stored on tapes and disks or spoken in conversation and over the telephone

- introducing a consistent approach to security ensuring that all employees and users fully understand their responsibilities

- creating and maintaining, within the organisation, a level of awareness of the need for information security as an integral part of daily business

- protecting information assets under the control of the College.

3. Scope

This policy applies to all information, information systems, networks, applications and locations in Caedmon College Whitby. Ultimate responsibility for information security rests with the Senior Information Risk Officer at the College but, on a day-to-day basis, the Information Security Officer and the Data Protection Officer shall be responsible for managing and implementing the policy and related procedures and associated policies.

4. Definitions

Information System (IS): an information system is defined as a system that requires the use of and the support of the College's ICT infrastructure and/or a system that stores or manipulates data and/or any system that requires on-going support from the ICT department; eg, CMIS/E portal.

System Owner (SO): the System Owner (SO) is the individual who has overall responsibility for an information system, its governance and usage. At the College, it is the MIS Manager.

System Administrator (SA); the System Administrator (SA) is responsible for the day to day maintenance of the system. This is separated from the system owner role and at the College it is the Network Manager.

System User (SU): individuals who access and use the information system and network to perform tasks defined within their access roles and privileges. At the College these are staff, visitors and students.

5. Risks

Non-compliance with this policy could have a significant effect on the efficient operation of the College and may result in financial loss and an inability to provide necessary services to our students.

The College is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to users of the College network, who may be held personally accountable for any breaches of information security for which they may be held responsible. The College shall comply with the following legislation and other legislation as appropriate

The Data Protection Act (1998)
The Data Protection (Processing of Sensitive Personal Data) Order 2000.
The Copyright, Designs and Patents Act (1988)
The Computer Misuse Act (1990)
The Health and Safety at Work Act (1974)
Human Rights Act (1998)
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000
Health & Social Care Act 2001
Health & Social Care Act 2008
EU Directive on Privacy and Electronic Communications (2006)
Mental Health Act 1983
Mental Health Act 2007
Equalities Act 2010
Electronic Communications Act 2000
Intellectual Property Act 1994

Other legal statutes brought into force after this document is printed will also apply without exception.

6 Applying the Policy

6.1 Management of Security

The Information Security Officer shall be responsible for implementing, monitoring, documenting and communicating security requirements for the College.

Line Managers are responsible for ensuring that their permanent and temporary staff are aware of:

- the information security policies applicable in their work areas
- their personal responsibilities for information security
- how to access advice on information security matters.

All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity.

The Information Security Policy shall be maintained, and updated by the Information Security Officer and reviewed by the College's Governing Body. This review shall take place annually and be recorded within the revision history of the policy

Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

Each member of staff shall be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force and identified within the policy, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

Contracts with external contractors that allow access to the College's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

6.2 Information Security Awareness Training

Information security awareness is included in the staff induction process. An ongoing awareness program ensures that staff awareness is refreshed and updated as necessary. Training is available to all staff by the ICT Department.

6.3 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage.

6.4 Security Control of Assets

Each user of IT assets (hardware, software, application or data) shall be responsible for the information security of that asset whilst logged on.

6.5 Access Controls

Only authorised personnel who have a justified and approved need shall be given access to restricted areas containing information systems or stored data.

6.6 User Access Controls

Access to information shall be restricted to authorised users who have a legitimate need to access the information.

6.7 Computer Access Control

Access to computer facilities shall be restricted to authorised users who have a need to use the facilities.

6.8 Application Access Control

Access to data, system utilities and programmes shall be controlled and restricted to those authorised users who have a legitimate need. Authorisation to use an application shall depend on the availability and procurement of a license from the supplier.

6.9 Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

6.10 Computer and Network Procedures

The College's ICT Department is responsible for ensuring that computers and networks are controlled and managed through standard documented procedures that have been authorised.

6.11 Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks shall be managed on a formal basis by ICT. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of the College's risk management programme. These reviews shall help identify areas of continuing best practice and possible weaknesses/potential risks that may have arisen since the last review was completed.

6.12 Information security incidents and weaknesses

All information security events and suspected weaknesses are to be reported to the Information Security Officer. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

6.13 Classification of Sensitive Information

A consistent system for the classification of information within government organisations enables common assurances in information partnerships, consistency in handling and retention practice when information is shared with non-government bodies

The College shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the Information Governance Toolkit to secure their information assets.

The Information Security Officer or Data Protection Officer should be contacted for further guidance and instruction.

6.14 Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the College's property without permission from the College ICT department.

6.15 User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the College's ICT department before they may be used on College systems. Such media must also be fully virus checked before being used on the College's equipment.

6.16 Monitoring System Access and Usage

An audit trail and log will be kept of all monitoring that is undertaken. The College has in place routines to regularly audit compliance with this and other policies. In addition it

reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons

- establishing the existence of facts
- investigating or detecting unauthorised use of the system
- preventing or detecting crime
- ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- in the interests of national security
- ascertaining compliance with regulatory or self-regulatory practices or procedures
- ensuring the effective operation of College systems.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act (1998).

6.17 Accreditation of Information Systems

The College shall ensure that all new information systems, applications and networks include a security plan and are approved by the College's ICT department before they commence operation.

6.18 System Change Control

Changes to information systems, applications or networks shall be reviewed in line with the change control policy. The College ICT Department must be involved in this process.

6.19 Intellectual Property Rights

The College shall ensure that all information products are properly licensed and approved by the College's ICT department. It is the responsibility of the system owner to work with the College's ICT department to ensure this takes place.

Users shall not install software on the College's property without permission from the ICT Department.

• 7. Policy Compliance

All users are required to comply with this policy in respect of its provisions and ethos. Failure to do so may be regarded as a breach of the Code of Conduct and could result in action being taken against the person concerned.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, you should seek advice from the Information Security Officer.

The College's ICT Department and the Information Security Officer shall keep the Strategic Team informed of the information security status of the College by means of regular reports and presentations of serious security breaches (eg, significant loss of data) will be reported to the Information Commissioners Office once approved by the Senior Information Risk Officer.

8. Policy Governance

The following table identifies who within the College is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	The Principal
Accountable	The Business Group / Senior Teacher
Consulted	NYCC, the Governing Body and staff
Informed	All College employees, temporary staff, contractors and students

Data Protection Officer (DPO)

Maintained schools and colleges, and academies, will require a DPO. (However, there is provision for a group of schools/colleges, for example, a multi-academy trust, to appoint a single DPO.) This officer can be an existing staff member (provided their other role does not result in a conflict of interest) and s/he will report to the highest level of management in your organisation. The DPO will have responsibility for:

- informing and advising the school/college and its employees about the requirements around data protection
- monitoring compliance with GDPR and other legal data protection requirements, including the organisation's policies relating to the same
- raising awareness and training staff
- related audits
- being the contact point for and co-operating with the Information Commissioner's Office (ICO)

This policy shall be subject to audit by internal and external auditors.

9. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months. Policy review will be undertaken by the Information Security Officer in consultation with the College Governing Body.

10. References

- Users shall not install software on the College's property without permission from the College's ICT Department

- All information security events and suspected weaknesses are to be reported to the Information Security Officer

- Each member of staff shall be responsible for the operational security of the information systems they use

- Only authorised personnel who have a justified and approved need shall be given access to restricted areas containing information systems or stored data.

Appendix 1

STANDARD COSTS TO BE USED IN THE CALCULATION OF FEES FOR REQUESTS UNDER THE FREEDOM OF INFORMATION ACT 2000

Staff time	£25.00 per hour
Photocopying costs	10p per copy
Printing costs	10p per copy
Postage costs	1st class at cost or original estimate, whichever is lesser
Other items such as relevant translation	

NYCC CHARGING REGIME

Fee is less than £5.00	No charge will be made
Cost of fee between £5.00 and £450.00	If the cost to service a request is estimated at between £5.00 and £450.00 (approximately 17 staff hours plus £25 disbursements) then a charge for non-staff costs as above will be made.
Cost of fee is over £450.00 (*)	If the cost to service a request is estimated to cost in excess of £450.00 (more than 17 staff hours plus £25 disbursements) then the full cost, including staff time at the above rate, will need to be charged.
Aggregation of Requests (**)	If two or more requests are received within 60 consecutive working days, for the same or similar information either from the same person or different persons who appear to be acting as part of a campaign, then the charges will be aggregated. Once the cost exceeds £450.00 then the full costs, including staff time, will need to be charged.
Mixed Requests	If a request is received in which the information is covered by more than one access to information regime then, for the purposes of calculating fees, it is necessary to separate out the constituent parts of the request to determine what fee may be charged. The above charging regime is applicable to the FOI element.

***Where the fee is calculated at over £450.00**

Section 16(1) requires the County Council to provide advice and assistance, "so far as it would be reasonable to expect the authority to do so, to persons who propose to make, or have made, requests for information"	Stage 1 – If the request is particularly wide-ranging, and therefore likely to be expensive to answer, the County Council must discuss this with the applicant to see if the question could be refined to a more manageable level to bring it below the £450 limit.
	Stage 2 – If after providing advice and assistance, as required under Section 16, the request is still over the appropriate limit the County Council can either turn the request down or answer the request and charge a fee.
	Or where the County Council decides to provide the information and charge a fee, and does not have other powers to do so, the County Council can charge on the basis of the costs outlined above, as well as the cost of informing the applicant whether the information is held and communicating the information to the applicant.

**Further detailed guidance is available on the Data Matters Intranet site.