Information Policy

Data Protection Officer | Sept 2026

Minsthorpe Community College: A place where everyone plays a part in strengthening our learning community through Motivation, Commitment & Care.

Minsthorpe
Community College

Contents

	Page
1. Introduction	2
2. Data Protection	3
3. Information Asset Register	4
4. Information Asset Owners	4
5. Training	5
6. Privacy Notices	5
7. Information Sharing	6
8. Data Protection Impact Assessments (DPIA's)	6
9. Retention Periods	6
10. Destruction of records	7
11. Third Party Data Processors	7
12. Access to Information	8
13. Data Subject Rights	10
14. Complaints	10
15. Copyright	11
Final Section	12

Section 1

Introduction

This policy is to ensure that Minsthorpe Community College complies with the requirements of the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA), Environmental Information Regulations 2004 (EIR) and Freedom of Information Act 2000 (FOIA), associated guidance and Codes of Practice issued under the legislation.

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.

This policy is the College's main information governance policy and addresses:

- Data Protection (including rights and complaints)
- Freedom of Information
- Information Asset Management

Information security, acceptable use of systems, records management and security incident reporting will be addressed in separate policies.

Section 2

Data Protection

Personal data will be processed in accordance with the requirements of the UK GDPR and in compliance with the data protection principles specified in the legislation.
The college 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 below:

Schools Data Protection Officer
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL

schoolsDPO@veritau.co.uk
01904 554025

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;

Section 3

Information Asset Register

The College must maintain 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.

Section 4

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 college 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.

Section 5

Training

The college will ensure that appropriate guidance and training is given to the relevant staff, governors, and other authorised college 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 provide the College with adequate training resources and guidance materials.

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

Section 6

Privacy Notices

Minsthorpe Community College 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 college's website in an easily accessible area.

A privacy notice for employees will be provided at commencement of their employment with the college. Specific privacy notices will be issued where the data subject requires more information about specific processing (e.g. college 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 college's Information Asset Register.

Section 7

Information Sharing

In order to efficiently fulfil our duty of education provision it is sometimes necessary for the college 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.

Section 8

Data Protection Impact Assessments (DPIA's)

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

Section 9

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.

The College has opted to adopt the retention schedule suggested by the Information and Records Management Society (IRMS).

Section 10

Destruction of records

Retention periods for records are recorded in the college'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:

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

Section 11

Third Party Data Processors

All third-party contractors who process data on behalf of the college 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.

Section 12

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 enquiries@minsthorpe.cc

The Vice Principal in charge of GDPR is responsible for:

- 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.

Requests received will be acknowledged within 5 college days. The Principal 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

We have adopted the Information Commissioner's model publication scheme for colleges 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. Any charges will be formulated taking into account the limits set by the legislation.

We will adhere to the required timescales, and requests will be answered within 20 college days.

Requests for information under the UK GDPR- Subject Access Requests should be made to enquiries@minsthorpe.cc

Any member of staff/governor may receive a request for an individual's personal information. Whilst the UK 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 college.

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 college to be satisfied of the applicant's identity;

Only once the college 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 requests within the statutory timescale of One Calendar Month.

The college can apply a discretionary extension of up a further two calendar months 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 calendar month 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 student in question.

Requests received from parents asking for information held within the student'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.

Section 13

Data Subject Rights

As well as a right of access to information, data subjects have a series of other rights prescribed by the UK 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 the DPO who will acknowledge the request and respond within one calendar month.

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.

Section 14

Complaints

Complaints in relation to data subject rights will be processed as an Internal Review request.

Requests for an Internal Review should be made within 40 working days from the applicant receiving of the original response. After that time, the college is not obliged to respond to the request for a review.

Any individual who wishes to make a complaint about the way we have handled their personal data should contact the college or our DPO on the address provided. The college will then review the original response to the request and decide whether it was handled appropriately.

Any other complaints about data protection related matters will be handled through our complaints procedure.

Section 15

Copyright

Minsthorpe Community College 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 college is not re-used in a way which infringes those interests, whether or not any such warning has been given.

Final Section

Equality Assessment

This policy has been assessed with regard to its impact on equalities issue, with specific reference to the aims of the Equality Act 2010. The equality impact assessment focused on race, gender, disability, pregnancy and maternity, age, sexual orientation, gender reassignment and religion/belief.

Updates

Sept 26 – minor updates

Policy Review Schedule

Policy last reviewed:	Due for next review:	Role Responsible:
September 2022	September 2024	Data Protection Officer
September 2024	September 2026	Data Protection Officer
September 2026	September 2028	Data Protection Officer