



Cookstown High School

Data Protection Policy

Reviewed: February 2024

Next Review: February 2027

Contents

POLICY OVERVIEW..... 3

RECORD OF POLICY AMENDMENTS 3

Ethos and Rationale..... 4

DATA PROTECTION POLICY..... 5

 Scope 5

 Data Protection Principles..... 5

 Lawful, Fair and Transparent Processing 6

 Rights of the Individual..... 6

Data Protection Officer 7

Privacy by Design..... 7

Data Retention & Disposal 8

Data Breach 8

Third-Party Services and Subcontracting 8

Complaints..... 8

Definitions 9

Monitoring and Review 9

Appendix 1..... 10

 GDPR Document Retention 10

POLICY OVERVIEW

DETAILS

TITLE	Data Protection Policy
TARGET AUDIENCE	Governors', Staff, Parents/Guardians
REVIEW DATE	February 2024
REVIEW LEAD	Principal
POLICY DEVELOPED BY	Senior Leadership Team
POLICY RATIFIED BY THE BOARD OF GOVERNORS ON:	February 2024
EFFECTIVE FROM:	February 2024
REVIEW FREQUENCY:	Every three years (minimum)
REVIEW DATE:	February 2027
PRINCIPAL	Miss G J Evans
CHAIR OF BOARD OF GOVERNORS	Mrs L Dripps

This procedure has been reviewed to include reference to the remit of the Northern Ireland Public Services Ombudsman (NIPSO) in investigating complaints from members of the public in relation to maladministration in publicly funded schools.

RECORD OF POLICY AMENDMENTS

The following table outlines any significant changes/amendments made to this procedure since it was ratified by the Board of Governors on:

DATE OF REVIEW OR AMENDMENT	SUMMARY OF CHANGED / AMENDMENTS TO PROCEDURE	AMENDED BY

Ethos and Rationale

At Cookstown High School we believe privacy is important. We are committed to complying with our data protection obligations and to being concise, clear and transparent about how we obtain and use Personal Information and how (and when) we delete that information once it is no longer required.

The school ethos values and respects the individual as unique while also emphasising the importance of responsibility and corporate life. This policy should be read, interpreted and applied in a manner consistent with the school ethos.

Any queries in relation to this policy or any of the matters referred to in it should be submitted to the Principal.

The following policies, procedures and documents are also relevant to this Policy:

Acceptable Use of the Internet Policy
Bring Your Own Device (BYOD) Policy
Concerns and complaints Procedure
Data Breach Management Procedure
Department of Education Document Disposal Schedule
Email Etiquette
Subject Access Request Procedure

DATA PROTECTION POLICY

Scope

The School is subject to the General Data Protection Regulation (GDPR) which imposes obligations on the School as a data controller in relation to the protection, use, retention and disposal of Personal Information. This Policy sets out the procedures that are to be followed when dealing with Personal Information and applies to all Personal Information processed by or on behalf of Cookstown High School.

You must read this Policy because it gives important information about:

- the data protection principles with which School must comply
- what is meant by Personal Information and Special Category Data
- how we gather, use and (ultimately) delete Personal Information and Special Category Data in accordance with the data protection principles
- where more detailed Privacy Information can be found, e.g. about the Personal Information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept
- your rights and obligations in relation to data protection
- the consequences of our failure to comply with this Policy

Please refer to the School's privacy notices which are available on the school website or by contacting the general office and, where appropriate, to other relevant policies including in relation to acceptable use of the internet, BYOD and the DE Disposal Schedule which contain further information regarding the protection of Personal Information in those contexts.

Data Protection Principles

GDPR sets out the following principles with which any party handling Personal Information must comply.

All Personal Information must be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes only, and will not be further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- accurate and, where necessary, kept up to date and take reasonable steps to ensure that inaccurate Personal Information are deleted or corrected without delay
- kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the information is processed; Personal Information may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of the individual
- processed in a manner that ensures appropriate security of the Personal Information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Lawful, Fair and Transparent Processing

The School will, before any processing of Personal Information starts for the first time, and then regularly while it continues:

- Process the Personal Information on at least one of the following bases:

Consent:

- the individual has given their express agreement to the processing of their Personal Information for one or more specific purposes
- parental consent will be obtained for any child aged under 13 years old

Contractual:

- the processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract

Legal Obligation:

- the processing is necessary for compliance with a legal obligation to which the School is subject

Vital Interests:

- the processing is necessary for the protection of the vital interests of the individual or another natural person

Public Interest:

- the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority

Legitimate Interests:

- the processing is necessary for the purposes of legitimate interests of the School or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the individual, in particular where the individual is a child
- Except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose)
- Document our decision as to which lawful basis applies to help demonstrate our compliance with the data protection principles
- Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices which are available on the school website or from the General Office
- Where Special Category Data is processed, identify a lawful special condition for processing that information and document it
- Where criminal offence information is processed, identify a lawful condition for processing that information and document it

Rights of the Individual

The GDPR states that individuals have the following rights in respect of the processing of their Personal Information:

The right to be informed:

- The School will keep individuals informed of its processing activities through its privacy notices which are available on the school website or from the general office.

The right of access:

- An individual may make a subject access request (“SAR”) at any time to find out more about the Personal Information which the School holds on them. All SARs must be forwarded to the Principal
- The School is required to respond to a SAR within one month of receipt but this can be

extended by up to two months in the case of complex and/or numerous requests and, in such cases, the individual will be informed of the need for such extension. The School does not charge a fee for the handling of a straightforward SAR

The right to rectification:

- If an individual informs the School that Personal Information held by the School is inaccurate or incomplete, the individual can request that it is rectified.

The right to erasure:

- An individual is entitled to request that the School ceases to hold Personal Information it holds about them
- The School is required to comply with a request for erasure unless the School has reasonable grounds to refuse

The right to restrict processing:

- An individual is entitled to request that the School stops processing the Personal Information it holds about them in certain circumstances

The right to data portability:

- An individual has the right to receive a copy of their Personal Information and use it for other purposes

The right to object:

- An individual is entitled to object to the School's processing of their Personal Information.

Rights in relation to automated decision making and profiling:

- An individual has the right to challenge any decision that is made about them on an automated basis (subject to certain exceptions)
- The School is also required to comply with certain conditions if it uses Personal Information for profiling purposes

Data Protection Officer

A Data Protection Officer (DPO) is appointed who will monitor adherence to this policy.

The DPO is the Education Authority (dpo@eani.org.uk). Tel: 02882 411300.

The DPO is required to have an appropriate level of knowledge.

Privacy by Design

- The School has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process Personal Information will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.
- The data protection impact assessment will include:
 - Consideration of how Personal Information will be processed and for what purposes
 - Assessment of whether the proposed processing of Personal Information is both necessary and proportionate to the purpose(s)
 - Assessment of the risks to individuals in processing the Personal Information
- What controls are necessary to address the identified risks and demonstrate compliance with legislation.
- A data protection impact assessment is conducted by the Principal:
 - On every business process periodically, at least once a year and more frequently where the amount and/or sensitivity of Personal Information processed, dictates so

- As part of the project calendar admission requirements checklist
- At every high-impact change, and/or at the request of the Data Protection Officer

Data Retention & Disposal

The longer that Personal Information is retained, the higher the likelihood is of accidental disclosure, loss, theft and/or information growing stale.

Any Personal Information kept by the School is managed in accordance with the Department of Education Disposal of Records Schedule (<https://www.education-ni.gov.uk/publications/disposal-records-schedule>) (Appendix 1)

Data Breach

A data breach is any (potential) unintended loss of control over or loss of Personal Information within the School's environment. Preventing a data breach is the responsibility of all the School staff and its workforce.

Please refer to the School's Data Breach Management Procedure.

Third-Party Services and Subcontracting

The School may decide to contract with a third party for the collection, storage or processing of data, including Personal Information such as GL Assessments.

If the School decides to appoint a third party for the processing of Personal Information, this must be regulated in a written agreement in which the rights and duties of the School and of the subcontractor are specified. A subcontractor shall be selected that will guarantee the technological and organisational security measures required in this Policy and provide sufficient guarantees with respect to the protection of the personal rights and the exercise of those rights.

The subcontractor is contractually obligated to process Personal Information only within the scope of the contract and the directions issued by the School.

Complaints

Complaints will be dealt with in line with the School's Concerns and Complaints policy which is available on the school website or from the General Office.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. The ICO's details are as follows:

The Information Commissioner's Office – Northern Ireland
3rd Floor
14 Cromac Place,
Belfast
BT7 2JB

Telephone: 028 9027 8757 / 0303 123 1114
Email: ni@ico.org.uk

Definitions

“consent”

is any freely given, specific and transparently, well-informed indication of the will of the individual, whereby the individual agrees that his or her Personal Information may be processed. Particular requirements about consent can arise from the respective national laws.

“Personal Information”

(sometimes known as “personal data”) means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly — in particular, by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

“processing”

means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with Personal Information.

“Special Category Data”

(sometimes known as “sensitive personal data”) means Personal Information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data and the processing of data concerning health or sex life

Monitoring and Review

The Board of Governors will monitor developments in data management and protection and will review and amend this policy as appropriate and in keeping with EA advice.

Appendix 1

GDPR Document Retention

Data held or collected by School	How long is data item kept? Or used for?
PUPIL DATA (WITHIN MIS)	
Pupil Records	DOB + 25 years
Welfare/Safeguarding/Child Protection Data	DOB + 25 years
SEN	DOB + 25 years
EAL	Part of pupil record
Exclusion, behaviour	Part of pupil record
Reports	Part of pupil record
Examination Results/ Statutory Assessments	Current year + 6 years
Attendance Registers	Date of Entry + 3 years
Student Photos	Part of pupil record
STAFF DATA (WITHIN MIS)	
Staff Personnel File	Termination of employment + 6 years
Performance / CDP data	Part of personnel file
Staff absence data	Part of personnel file
Staff photos	Part of personnel file
OTHER PERSONNEL DATA	
Recruitment of new staff	Date of recruitment + 6 years
DBS / vetting checks	Note of proof on personal file/physical copies > 6 months
Appraisal /CPD data	Current year + 5 years
Disciplinary and grievance records	Date of warning + 6-18 months (take advice)
Allegation of a child protection matter	Until retirement (or 10 years from allegation if longer) (take advice)
Malicious allegation of a child protection matter	Dispose at end of case (take advice)
Health & Safety assessments	Date of meeting + 3 years (then review)
Health & Safety Accident Reports	Take advice - depends on nature of incident
Admissions papers (successful/unsuccessful)	Date of admissions/case resolution + 1 year
Student medical records/reports	DOB + 25 years

Student social services records and reports	DOB + 25 years
Financial Matters	
Annual Accounts	Current year + 6 years
Purchase Orders / Invoices / Payments	Current year + 6 years
Records around budget management	Current year + 3 years
Asset Management	Current year + 6 years
School Fund	Current year + 6 years
FSM* - Free School Meals Registers	Current year + 6 years
School Meals Registers	Current year + 3 years
Records relating to School Lettings	Current year + 6 years
Access Control / Passwords* into Systems	
Authorise data access / Nominated Contacts	Until changes in personnel or in-line with passwords policy
Network administration / Password Lists	Until changes in personnel or in-line with passwords policy
Email Management	Until changes in personnel or in-line with passwords policy
Web Filtering Management - Websense	Until changes in personnel or in-line with passwords policy
School Website Administration	Until changes in personnel or in-line with passwords policy
Social Media Platforms (Twitter, etc.)	Until changes in personnel or in-line with passwords policy
Learning Platform password information	Until changes in personnel or in-line with passwords policy
Communications	
Information added to website	Until changes in personnel or in-line with password policy
Information added to social media	Until changes in personnel or in-line with password policy
Learning Platform content	Until changes in personnel or in-line with password policy
Parental messaging system correspondence	Date of correspondence + 3 years
Back-up media (where on site)	Daily back-ups with back-up to one year
Back-up media in Cloud	Check Cloud providers' retention & deletion criteria
Emergency mobile phone loaded with data	Whilst staff in school and numbers valid
Governors	
Governors' documents with sensitive content	Date of meeting + 10 years

Governors' standard published meeting documents	Date of meeting + 6 years
Reports presented to Governors meeting	Date of meeting + 6 years
Annual Governors reports	Date of meeting + 10 years
Annual parents' meeting papers	Date of meeting + 6 years
Policies and plans administered by Governing body	Life of policy + 3 years
Other T&L potentially sensitive material (List not exhaustive)	
Student photos (not required for pupil record)	Relevant life of the photo / annual housekeeping
Staff photos* (not required for Personnel record)	Relevant life of the photo / annual housekeeping
Early Years assets (not in core MIS)	Current year + 6 years
Student reports (not in core MIS)	Current year + 6 years
Student assessments (not in core MIS)	Current year + 6 years
Third Party comparative performance data	Current year + 6 years
Other Operational Potentially Sensitive Material (list not exhaustive)	
CCTV saved footage	90 days
Visitor signing-in book / management system	Current year + 6 years / review
Biometric system - registration	Date of entry + 3 years
Newsletters/information with short operational life	Current year + 1 Year