Burnside College

Data Protection Policy

2026

Reviewed by DPW - May 2026
Ratified by Governors - July 2026

DATA PROTECTION POLICY

1.0 Introduction

Burnside College Data Protection Policy has been produced to ensure compliance with the General Data Protection Regulation (GDPR) and associated legislation, and incorporates guidance from the Information Commissioner's Office (ICO).

The Data Protection Policy gives individuals rights over their personal data and protects individuals from the erroneous use of their personal data.

Burnside College is registered with the ICO as a Data Controller for the processing of living individuals' personal information. ICO registration number: Z747445X

2.0 Purpose

Burnside College Data Protection Policy has been produced to ensure its compliance with the UK GDPR.

The Policy incorporates guidance from the ICO, and outlines the School's overall approach to its responsibilities and individuals' rights under the data protection legislation.

3.0 Scope

This Policy applies to all employees (including temporary, casual or agency staff and contractors, consultants and suppliers working for, or on behalf of, the School), third parties and others who may process personal information on behalf of the School.

The Policy also covers any staff and pupils who may be required to process or have access to personal data, for instance as part of a research project or as part of professional practice activities. If this occurs, it is the responsibility of the School to ensure the data is processed in accordance with the UK GDPR and that pupils and staff are advised about their responsibilities.

4.0 Data covered by the Policy

A detailed description of this definition is available from the ICO, however briefly; personal data is information that relates to an individual and the individual can be identified or identifiable either directly or indirectly from one or more identifiers or from factors specific to the individual. This includes data held manually and electronically and data compiled, stored or otherwise processed by the School, or by a third party on its behalf.

Special category data is personal data that is more sensitive in nature and requires a higher level of protection. This consists of information relating to:

- race;
- ethnic origin;

- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;

- sex life; or
- sexual orientation.

5.0 The Seven Data Protection Principles

UK GDPR requires Burnside College, its staff and others who process or use any personal information to comply with the seven data protection principles.

The principles require that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

g) accountability, the controller shall be responsible for, and be able to demonstrate compliance with the above.

6.0 Responsibilities

Burnside College has an appointed Data Protection Officer to handle day-to-day issues which arise, and to provide members of the School with guidance on Data Protection issues to ensure they are aware of their obligations.

All new staff will be required to complete mandatory information governance training as part of their induction and existing staff will be required to undertake refresher training on a regular basis.

Employees of Burnside College are expected to:

- Familiarise themselves and comply with the seven data protection principles.
- Ensure any possession of personal data is accurate and up to date.
- Ensure their own personal information is accurate and up to date.
- Keep personal data for no longer than is necessary inline with retention guidelines.
- Ensure that any personal data they process is secure and in compliance with Burnside College's information related policies and strategies.

- Acknowledge data subjects' rights (e.g. right of access to *all* their personal data held by Burnside College) under UK GDPR, and comply with access to those records.
- Ensure personal data is only used for those specified purposes and is not unlawfully used for any other business that does not concern Burnside College.
- Obtain consent when collecting, sharing or disclosing personal data.
- Contact dpo.schools@northtyneside.gov.uk for any concerns or doubt relating to data protection to avoid any infringements of the data protection legislation.

Pupils, of Burnside College are expected to:

- Comply with the seven data protection principles
- Comply with any security procedures implemented by Burnside College.

7.0 Obtaining, Disclosing and Sharing

Only personal data that is necessary for a specific School related business reason should be obtained.

Pupils and their parents and or Carers will be informed about how their data will be processed.

Upon acceptance of employment at Burnside College, members of staff will also be informed about the processing and storage of their data which is required as part of their legal contract and employment legislation.

Data must be collected and stored in a secure manner.

Personal information must not be disclosed to any third party organisation without prior consent of the individual concerned. This also includes information that would confirm whether or not an individual is or has been an applicant, pupil or employee of Burnside College. The only exception to this is where Burnside College has safeguarding concerns (please see paragraph 9)

Burnside College may have a duty to disclose personal information in order to comply with legal or statutory obligations. UK GDPR allows the disclosure of personal data to authorised bodies, such as the police and other organisations that have a crime prevention or law enforcement function.

Personal information that is shared with third parties on a more regular basis shall be carried out under written agreement to stipulate the purpose and boundaries of sharing. For circumstances where personal information would need to be shared in the case of ad hoc arrangements, sharing shall be undertaken in compliance with the data protection legislation.

8.0 Retention, Security and Disposal

Those responsible for the processing and management of personal data need to ensure that the data is accurate and up-to-date. If an employee, student or applicant is dissatisfied with the accuracy of their personal data, then they must inform the Director of Support Services.

Personal information held in paper and electronic format shall not be retained for longer than is necessary. In accordance with Article 5 of the UK General Data Protection Regulations,

personal information shall be collected and retained only for business, regulatory or legal purposes.

In accordance with the provisions of the UK GDPR, all staff whose work involves processing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage and ensure appropriate measures are in place to prevent accidental loss or destruction of, or damage to, personal data.

Burnside College's staff working from home, they will be responsible for ensuring that personal data is stored securely and is not accessible to others.

All data past its retention period should be destroyed in accordance with the Retention Schedule when it is no longer required.

Personal data in paper format must be shredded or placed in the confidential waste bins provided. Personal data held in electronic format should be deleted. Hardware or any digital storage should be appropriately disposed of in compliance with your ICT service provider contract and conform with UK GDPR requirements.

The four categories of retention periods to be applied to data are as follows:

a. One month after the creation of the data, to ensure any 'loose ends' are tied up.

b. One year after the pupil to whom the data relates leaves Burnside College, in order to ensure smooth handover activity to any subsequent school.

c. Five years after the pupil to whom the data relates leaves Burnside College, to support longer term analysis of progress, attainment, support for different pupil groups etc.

d. Until the child is 25 years of age or older, in instances where detailed information about activities in school may form part of safeguarding for that individual.

Where Burnside College decides to retain data for 5+ years, it will take steps to de-personalise it as time goes on. For example, names can be replaced with initials or other pseudonymisations.

9.0 Safeguarding

UK GDPR does not prevent the sharing of information for the purposes of keeping children safe. The Data Protection Act 2018 allows for schools to process sensitive information without consent where there are safeguarding concerns.

If Burnside College decides to share information for safeguarding purposes, the Designated Safeguarding Leads must record who they are sharing the information with and for what reason. If it is appropriate to do so, they should seek the consent of the data subject. If consent is not sought, this decision must be recorded.

10.0 Transferring Personal Data

Any transfer of personal data must be done securely in line with Burnside College's Information Security Policy.

Email communication is not always secure and sending personal data via external email should be avoided unless it is encrypted with a password provided to the recipient by separate means.

Care should be taken to ensure emails containing personal data are not sent to unintended recipients. It is important that emails are addressed correctly and care is taken when using reply all or forwarding or copying others into emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.

Personal email accounts should not be used to send or receive personal data for work purposes.

11.0 Data Subjects Right of Access (Subject Access Requests)

Under the GDPR, individuals (both staff and pupils) have the right of access to their personal data held by Burnside College. This applies to data held in both paper and electronic format, and within a relevant filing system.

Burnside College shall use its discretion under UK GDPR to encourage informal access at a local level to a data subject's personal information, but it will also have a formal procedure for the processing of Subject Access Requests.

Any individual who wishes to exercise this right should make the request in writing by contacting the Director of Support Services (D Paylor Wright).

Burnside College will not charge a fee. It will only release information upon receipt of a written request along with proof of identity or proof of authorisation where requests are made on behalf of a data subject by a third party. The requested information will be provided within the statutory timescale of 1 month from receipt of the necessary documentation.

12.0 The Education (Pupil Information) (England) Regulations 2005 – Information Request

Under education regulations, those with parental responsibility can request access to a child's education record. Access to education records is a separate right and is not covered by Data Protection legislation.

An education record covers information that comes from the school, the pupil or the parent, and is processed by or for the school's governing body or teacher. This is likely to cover information such as the records of the pupil's academic achievements as well as correspondence from teachers, local education authority employees and educational psychologists engaged by the school's governing body. It may also include information from the child and parent, carer or guardian.

Information provided by the parent of another child or information created by a teacher solely for their own use would not form part of a child's education record.

Those with parental authority will be able to view the record free of charge within 15 school days of the request.

If there is a request for a copy of the record, we can charge a fee for this, however, the fee will not exceed the cost of supplying the records. This will also be provided within 15 school days

13.0 Reporting a Data Security Breach

It is important Burnside College responds to a data security breach quickly and effectively. A breach may arise from a theft, a deliberate attack on School systems, unauthorised use of personal data, accidental loss or equipment failure. Any data breach should be reported to the Data Protection Officer at dpo.schools@northtyneside.gov.uk and if it relates to an IT incident (including information security), should also be reported to the Headteacher and in certain circumstances to your ICT provider – please refer to the Data Breach reporting policy for more information.

Any breach will be investigated in line with the procedures within the UK GDPR. In accordance with that Policy, Burnside College will treat any breach as a serious issue. Each incident will be investigated and judged on its individual circumstances and addressed accordingly.