Approved by:	Pat Kerton Chair of Governors	**Date:** March 2023
Last reviewed on:	March 2022	
Next review due by:	March 2024	

PRIVACY POLICY

High Close School

Contents

1. Aims

Our school aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 1998.

This policy applies to all data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the Data Protection Act 2018. The Education (pupil information) regulations 2015 and 2016 in addition to 2005 and is based on guidance published by the Information Commissioner's Office

It also takes into account the provisions of the General Data Protection Regulation

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed

Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. Data protection principles

The Data Protection Act 1998 is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

5. Roles and responsibilities

The trustees of Barnardo's have overall responsibility for ensuring that the school complies with its obligations under the Data Protection Act 1998.

Day-to-day responsibilities rest with the Principal, or the Senior Staff in the Principal's absence. The DPO will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

6. Privacy/fair processing notice

6.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information

- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.

Once our pupils reach the age of 13, we are legally required to pass on certain information to the local authority or youth support services provider in your area, which has responsibilities in relation to the education or training of 13-19 year-olds. Parents, or pupils if aged 16 or over, can request that only their name, address and date of birth be passed to the local authority or youth support services provider.

We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

6.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Performance Management Information
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to. Any staff member wishing to see a copy of information about them that the school holds should contact the Deputy Principal.

7. Subject Access Requests (SAR)

Under the Data Protection Act 1998, pupils and staff have a right to request access to information the school holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing to the Principal, either by letter, email or fax. Requests should include:

- The pupil's/staff members name
- A correspondence address

- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child
- The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.
- The school reserves the right to refuse to comply with a subject access request if it is determined to be 'manifestly unfounded or excessive'

8. Parental requests to see the educational record

Parents have the right of access to their child's educational record, free of charge, within 15 school days of a request. An education record covers information that comes from a teacher or other employee of a local authority or school, the pupil or you as a 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 from you, as a 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.

Access to education records is a separate right and is not covered by Data Protection legislation. Unlike the right to access under Data Protection legislation, this right does not extend to pupils.

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.

A parent may make a subject access request on their child's behalf, a subject access request is different to asking for the educational record. Please see section 9 of this policy

Primary

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may be granted without the express permission of the pupil.

Secondary

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may not be granted without the express permission of the pupil, however, each case will be considered on an individual basis.

Third Parties requests

An individual can make a subject access request via a third party. You should ensure that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

If it is thought that the individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, the response may be sent directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

9. Responding to a Subject Access Request

When a Subject Access Request is received we will acknowledge receipt of the SAR and inform the person submitting the request who will be managing their request. A person of suitable seniority, most likely the Deputy Principal, must be identified to manage the SAR; they may delegate appropriate tasks but the overall responsibility remains with them.

The request must be adhered to within 1 month of the notification, however, more time (up to 2 additional months) may be used. If more time is required this must be communicated in writing within the first month.

If the request is sent to the school during the school holidays while to school is closed, the request will be responded to when the school reopens, this may be more than 1 month in the summer break.

The SAR Manager may ask for clarification of which data is specifically needed for the request. This may include:

- a request for a comprehensive list of what personal data you want to access, based on what you need;
- any details, relevant dates, or search criteria that will help the school identify what you want
- how you would like to receive the information eg Digital or hard copy

All information held by the school, relating the access request, will be collected including electronic and paper records, photographs, video and audio recordings. This includes any emails held about the subject.

Review the records and identify any information that must be redacted, such as information about a third party. Identify any information that may be harmful to the subject of the data if it is shared with them. Discuss this with SLT to decide whether there are sufficient grounds not to share the information (see section 7 for exceptions).

Agree with the data subject how the data will be shared (face-to-face, email, post, etc). Ensure that the data is sent securely.

Consider whether you need to talk through any of the data before it is shared, eg, could the data be harmful, does any of the data need qualifying, could it have a detrimental impact on the individual or their family.

If the subject identifies factual inaccuracies in core data amend the record. Personal data may not be inaccurate if it faithfully represents someone's opinion about an individual, even if the opinion proves incorrect. In these circumstances, the data would not need to be "corrected", but a note must be added stating that the subject disagrees with the opinion

Subject Access Requests are reported and reviewed using Onetrust.

10. Guidance on Redaction

To redact means to remove or delete information from a record. It can be deleted electronically or it can be concealed using redaction tape, concealer fluid or a marker pen and the page photocopied. Particularly when relying on marker pen, which often does not fully conceal text even after photocopying, it is important to check the final redaction to ensure that none of the redacted information is visible.

We are required to provide the information, not the documents. If it is easier to extract the information from a document this may be done, if it is included in a report concerning a number of different people for example, but if information is being withheld about the subject this must be indicated and the document or report should include a brief note explaining the redaction.

It should be noted that, although redaction of certain information is permitted, it is not acceptable to amend or delete data where there is no reason for redacting unless the data has otherwise been amended or deleted in the ordinary course of business

11. Storage of records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office
- Passwords must meet the requirements the network to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment

12. In the Event of a Data Breach

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. It is a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Disclosing information to someone within Barnardo's that shouldn't see it, or someone in Barnardo's accessing information that they shouldn't, is still a breach, and should be reported. It is important to report a data breach to your line manager or Data Protection Manager as soon as you become aware of it. Even if you just suspect there has been a breach you should still report it.

The Data Protection Manager for High Close School is Wendy Gosling, Deputy Principal.

Data Breaches are recorded and reviewed using OneTrust.

The decision about whether to report a breach to the Information Commissioner's Office (ICO) is determined by Barnardo's Data Protection Officer (DPO) in discussion with the appropriate Data Protection Manager (DPM) after an investigation. However, if we decide we don't need to report the breach, we need to be able to justify this decision, so should document it. We have to make these decisions quickly because we only have 72 hours from discovering the breach to report it to the ICO, this includes evenings and weekends. So, if we discover the breach at 3pm on a Friday evening, and it's a serious one, we've only got until 3pm on Monday to report it.

The UK General Data Protection Regulation (UK-GDPR) recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Therefore, Article 34(4) allows us to provide the required information in phases, as long as this is done without undue further delay.

13. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. We will shred paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records.

14. Training

Our staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary.

15. Monitoring arrangements

The Barnardo's Data Protection Officer, Martine King, is responsible for and has oversight of all processes regarding data protection. The Data Manager checks that the school complies with this policy by, among other things, reviewing school records every half year

This document will be reviewed **every 2 years**. At every review, the policy will be shared with the governing board.