Brookfield School

DATA PROTECTION POLICY

Version	Date Reviewed	Reviewed by	Next Review Date
TBC	September 2019	Fiona Carver	TBC

Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

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

1.1 The School is required to process personal data collected relevant to its operation and shall take all reasonable steps to do so in accordance with this Policy.

In this Policy any reference to pupils, parents, friends or staff includes current past or prospective pupils, parents, friends or staff.

1.2 All staff are responsible for complying with this policy.

2. SCOPE

2.1 This Policy covers the School's acquisition, handling and disposal of the personal and sensitive personal data it holds on all Staff, including temporary staff, agency workers, volunteers, parents and pupils. It also applies to Governors and contractors.

It explains the School's general approach to data protection, which is to ensure that individual's personal data and information is protected and appropriately processed and provides practical guidance, which will help to ensure that the School complies with the Data Protection Act 2018 (the Act), and the General Data Protection Regulations 2018 (GDPR) which became law on 25th May 2018.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: * Name (including initials) * Identification number * Location data * Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: * Racial or ethnic origin * Political opinions * Religious or philosophical beliefs * Trade union membership * Genetics * Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes

	* Health – physical or mental * Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed
Data controller	A personal or organisation that determines the purposes of processing of personal data
Data processor	A personal or other body, other than an employee or the data controller, who processes personal data on behalf of the data controller
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data

4 The Data Controller:

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

As the Data Controller the School is responsible for complying with the Act.

The Data Protection Officer: The School has appointed Mrs. Claire Goksu as its Data Protection Officer, responsible for day-to-day compliance with this Policy. She can be contacted at goksuc@brookfield56.lancs.sch.uk.

5. ACQUIRING, USING AND DISPOSAL OF PERSONAL DATA

The School shall only process personal data for specific and legitimate purposes. These are:

a) providing pupils and staff with a safe and secure environment including images on CCTV – all cameras around the School carry appropriate warning signs as to their operation. They are used for the purpose of detecting crime, ensuring personal security and the welfare of staff and pupils and the protection of the working environment. Images are kept no longer than 14 days to meet these objectives, however, in certain circumstances such as an on-going investigation into criminal activity certain relevant images may be kept for longer but no longer than necessary to complete any such investigation.

Commented [o1]: Need to discuss the element of CCTV and whether school uses/has it

b) providing an education, training and pastoral care.

c) providing activities for pupils and parents - this includes school trips and activity clubs.

d) providing academic, examination and career references for pupils and staff.

e) protecting and promoting the interests and objectives of the School – this includes fundraising.

f) safeguarding and promoting the welfare of pupils.

g) monitoring pupils' and staff's email communications, internet and telephone use to ensure pupils and staff are following the **School's E-Safety and Acceptable Use policy.**

Commented [o2]: Rename with the appropriate titled policies referenced

h) promoting the School to prospective pupils and their parents.

i) communicating with former pupils.

j) for personnel, administrative and management purposes. For example to pay staff and to monitor their performance.

k) fulfilling the School's contractual and other legal obligations.

Staff should seek advice from the Data Protection Officer before using personal data for a purpose which is different from that for which it was originally acquired. If information has been obtained in confidence for one purpose, it shall not be used for any other purpose without the Data Protection Officer's permission.

The School shall not hold unnecessary personal data, but shall hold sufficient information for the purpose for which it is required. The School shall record that information accurately and shall take reasonable steps to keep it up-to-date. This includes an individual's contact and medical details.

The School shall not transfer personal data outside the European Economic Area (EEA) without the data subject's permission unless it is satisfied that the data subject's rights under the Act will be adequately protected and the transfer has been approved by the Data Protection Officer. This applies even if the transfer is to a pupil's parents or guardians living outside the EEA.

When the School acquires personal information that will be kept as personal data, the School shall be fair to the data subject and fair to whoever provides the information (if that is someone else) in that their data will be handled and safeguarded in compliance with the Act.

The School shall only keep personal data for as long as is reasonably necessary. The school has adopted use of the IRMS Toolkit. Staff should not delete records containing personal data without authorisation.

The School will keep personal data secure and adopt technical and organisational measures to prevent unauthorised or unlawful processing of personal data.

6. INFORMATION AND EXPLANATION

Individuals must be told what data is collected about them, and what it is used for.

This is called a privacy notice or statement.

Purpose: The privacy notice is to ensure that the School's collection and processing of personal data is done in a transparent way so it will explain who it applies to, why the information is being collected, what information will be collected, how it will be acquired and processed, what it will be used for, which third parties (if any) it will be shared with, how long records will be retained for and outline the data subject's rights, including the right to complain about the processing of their data to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow. Cheshire SK9 5AF, telephone 0303 123 1113 or at: https://ico.org.uk/concerns/

Version	Date Reviewed	Reviewed by	Next Review Date
TBC	September 2019	Fiona Carver	TBC

Staff are not expected to routinely provide pupils, parents and others with a privacy notice as this should have already been provided. Copies of the School's privacy notice for pupils and parents can be obtained from the Data Protection Officer or accessed on the School's website.

Use: Having said this, staff should inform the Data Protection Officer if they suspect that the School is using personal data in a way that might not be covered by an existing privacy notice. This may be the case where, for example, staff are aware that the School is collecting medical information about pupils without telling their parents what that information will be used for.

7. PROTECTING CONFIDENTIALITY

Disclosing personal data within the School: Personal data should only be shared on a need to know basis. Personal data shall not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority within the School or their relationship to the data subject, unless they need to know it for a legitimate purpose. Examples include - personal contact details for a member of staff (e.g. their home address and telephone number, and their private mobile telephone number and e-mail address) shall not be disclosed to parents, pupils or other members of staff unless the member of staff has given their permission.

Disclosing personal data outside of the School: Sharing personal data with others is often permissible so long as doing so is fair and lawful under the Act. However, staff should always speak to the Data Protection Officer if in doubt, or if staff are being asked to share personal data in a new way.

Before sharing personal data outside the School, particularly in response to telephone requests for personal data staff should:

a) make sure they are allowed to share it – that they have the necessary consent;

b) ensure adequate security. What is adequate will depend on the nature of the data. For example, if the School is sending a child protection report to social services on a memory stick then the memory stick must be encrypted; paper information should be sent by courier or recorded delivery, First or Second Class post is not considered secure enough,

c) make sure that the sharing is covered in the privacy notice.

The School should be careful when using photographs, videos or other media as this is covered by the Act as well. Our Home School Agreement requests parental permission as to the usage of photographs, videos and other media.

Information security and protecting personal data: Information security is the most important aspect of data protection compliance and most of the fines under the Act for non-compliance relate to security breaches. The School shall do all that is reasonable to ensure that personal data is not lost or damaged, or accessed or used without proper authority, and the School shall take appropriate steps to prevent these events happening. In particular:

a) paper records which include confidential information shall be kept in a cabinet or office which is kept locked when unattended.

b) the School uses a range of measures to protect personal data stored on computers, including file encryption, anti-virus and security software, sufficiently robust and frequently changed user passwords, audit trails and back-up systems.

c) staff must not remove personal data from the School's premises unless it is stored in an encrypted form on a password protected computer or memory device. Further information is available from the Data Protection Officer.

d) staff must not use or leave computers, memory devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons: they should not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased.

8. DATA BREACHES

Definition: A data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure or access to personal data.

Reporting obligations: Any actual data breach or alleged data breach must be reported to the Data Protection Officer as soon as it is discovered, whatever time that might be, to enable its circumstances to be investigated and appropriate action taken to limit any damage and to prevent a similar occurrence. As soon as the School becomes aware of a significant data breach as determined by the Data Protection Officer it has 72 hours in which to report the breach to the Information Commissioner's Office.

Examples of breaches and their seriousness for reporting purposes are:

a) mistakenly sending an email or letter containing personal data to an incorrect recipient.

b) theft of IT equipment containing personal data.

c) failing to deal with a Subject Access Request.

d) a discussion away from school where the individuals concerned are identifiable

If a breach is found to be sufficiently serious i.e. if not dealt with it is likely to result in a high risk to the rights and freedoms of individuals, e.g. resulting in discrimination, damage to reputation, financial loss – through identity theft or otherwise – loss of confidentiality or any other significant economic or social disadvantage, then not only does this breach have to be reported to the ICO within 72 hours of its discovery, the individuals concerned must be notified of the breach in a timely manner as directed by the Data Protection Officer.

9. DATA SUBJECT'S RIGHTS, INCLUDING ACCESSING ANY DATA HELD ON THEM

Individuals are entitled to know whether the School is holding any personal data that relates to them, what that information is, the source of the information, how the School uses it and who it has been disclosed to. This is known as a Subject Access Request. Any member of staff wishing to exercise the right to request information covered by this policy, can do so by submitting a request in writing to the Data Protection Officer. Any member of staff who receives a request for information covered by this policy from a pupil, parent or any other individual must inform the Data Protection Officer as soon as is reasonably possible, normally on the same day. This is important; as there is a statutory procedure and timetable, the School must follow. Information must be provided to the requestor without delay and at the latest within one month of receipt.

A) Individuals have a right to ask the School not to use their personal data for direct marketing purposes or in ways which are likely to cause substantial damage or distress.

B) Individuals have a right to ask for incorrect personal data to be corrected or annotated.

C) Individuals have the right to object to any of their personal data being processed and to have this data erased.

D) Individuals have the right to restrict (halt) the processing of their personal data, usually whilst incorrect data is being corrected.

E) Individuals have the right to request their personal data is transferred to another data controller in a commonly used format.

F) Individuals have a right to ask the School not to make automatic decisions (using personal data) if such automatic decisions would affect them to a significant degree.

G) Individuals have the right to complain about the processing of their personal data to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, Telephone 0303 123 1113 or at: https://ico.org.uk/concerns/.

10. DATA PROCESSORS

9Where the school uses data processors (third parties / organisations that process (deals with or stores) personal data on the school's behalf), the GDPR makes written contracts between the school and the processor a general requirement and that the contract must include certain specific terms as a minimum. If the data processor then (with the school's written authority) employs another processor, it also needs to have a written contract in place. The school will check all existing contracts and if they do not contain all the requirements it will get new contracts drafted and signed as required. The school will ensure data processors are communicated with so they understand :

a) the reasons for the changes;

b) the new obligations that GDPR put on them; and

c) that they may be subject to administrative fines or other sanctions if they do not comply with new obligations.

11. FURTHER INFORMATION

The School has registered its use of personal data with the Information Commissioner's Office and further details of the Personal Data it holds, and how it is used, can be found in the School's register entry on the Information Commissioner's website at www.ico.gov.uk under registration number ZA499394. This website also contains further information about data protection.

Further information and guidance regarding this policy or its application can be obtained from the Data Protection Officer.

12. BREACH OF THIS POLICY

Version	Date Reviewed	Reviewed by	Next Review Date
TBC	September 2019	Fiona Carver	TBC

11.1 A member of staff who deliberately or recklessly discloses personal data held by the School without proper authority is guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

13. STATUS

12.1 This policy is intended only as a statement of School policy. It does not form part of the contract of employment and may be amended from time to time.

13. RELATED POLICIES –

for example:

Behaviour & Discipline Policy

E-Safety and Acceptable Use Policy

School Workforce Privacy Notice for Staff

Staff Code of Conduct

Privacy Notice for Pupils and Parents

Document Retention Policy – IRMS toolkit

Data Breach Policy and Procedure

Subject Access Request Procedure

Commented [o3]: Alter to the appropriate name if necessary

Commented [o4]: To finalise policy for formality

Version	Date Reviewed	Reviewed by	Next Review Date
TBC	September 2019	Fiona Carver	TBC