Windmill Hill Primary School

GDPR Policy

1. INTRODUCTION

1.1 The School is required to process personal data regarding staff, pupils and their parents and guardians and friends of the School relevant to its operation and shall take all reasonable steps to do so in accordance with this Policy. Processing may include: obtaining, recording, holding, handling, disclosing, transportation, destroying or otherwise using data. 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 members 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 1998 (the Act) and anticipates the General Data Protection Regulations 2018 (GDPR) which become law on 25thMay 2018.

3. DEFINITIONS

3.1 Personal data is:

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

3.2 Sensitive personal data is:

Any information about a person's mental or physical health or condition, their political or religious beliefs, race, ethnicity, sexual life or orientation, trade union membership, criminal offences or alleged offences and any proceedings. The GDPR refers to sensitive personal data as "special categories of personal data". The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual

The School has additional obligations in connection with the use of sensitive personal data, namely at least one of the following conditions must be satisfied:

a) Explicit consent of the data subject must be obtained
b) Necessary for carrying out the obligations under employment, social security or social protection law or a collective agreement
c) Used in connection with alumni relations provided it relates solely to this and there is no disclosure to a third party without consent
d) Data manifestly made public by the data subject
e) Various public interest situations as outlined in the General Data Protection Regulations 2018

3.3 The Data Subject is:

The person the information relates to. There may be more than one data subject, such as when a record concerns an incident involving two pupils.

3.4 The Data Controller:

The School is the Data Controller and is responsible for determining the purposes of its use of data - what data it gathers and how this information is used. As the Data Controller the School is responsible for complying with the Act.

3.5 The Data Protection Officer:

The School has appointed Jonathan Greenough (Halton Borough Council) as its Data Protection Officer, responsible for day to day compliance with this Policy. He can be contacted by telephone on 0151 511 7002 or email **jonathan.greenough@halton.gov.uk**

4. ACQUIRING, USING AND DISPOSAL OF PERSONAL DATA

4.1 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.
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 members are following the School's IT Acceptable Use policy.
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 schools contractual and other legal obligations.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 The school shall only keep personal data for as long as is reasonably necessary and in accordance with the retention and disposal guidelines set out in the School's Document Retention Policy. Staff should not delete records containing personal data without authorisation.

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

5. INFORMATION AND EXPLANATION

5.1 Privacy Notice: Individuals must be told what data is collected about them, and what it is used for. This is called a privacy notice or statement.

5.2 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/.

5.3 Staff members 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.

5.4 Use: Having said this, staff should inform the Data Protection Officer if they suspect that the School is using personal data in a way which 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 I information about pupils without telling their parents what that information will be used for.

6. PROTECTING CONFIDENTIALITY

6.1 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.

6.2 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 members are being asked to share personal data in a new way.

6.3 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 and

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

6.4 The school should be careful when using photographs, videos or other media, as this is covered by the Act as well.

6.5 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 members 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 members 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.

7. DATA BREACHES

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

7.2 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.

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.

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

8.1 Individuals are entitled to know whether the school is holding any personal data which 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 which the school must follow. Information must be provided to the requestor without delay and at the latest within one month of receipt.

8.2 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.

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

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

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

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

8.7 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.

8.8 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/.

9. DATA PROCESSORS

9.1 Where 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:

- the reasons for the changes;
- the new obligations that GDPR put on them; and
- that they may be subject to administrative fines or other sanctions if they do not comply with new obligations.

New and existing contracts must comply with GDPR by 25th May 2018.

10. FURTHER INFORMATION

10.1 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 Z6504960

This website also contains further information about data protection.

11. BREACH OF THIS POLICY

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.

12. 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 and Discipline Policy

Acceptable Use of ICT and the Internet Policy

Privacy Notice

Privacy Notice for Pupils

Document Retention Policy

14. FURTHER INFORMATION

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