Policy for # Data Protection Policy (2019)		
Date of policy:	August 2019	Committee: Full Governing Body
Next review:	August 2021 (Review Period 2 Years)	

Contents

INTRODUCTION

The School is required to process personal data regarding staff, students 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 students, parents, friends or staff includes current past or prospective students, parents, friends or staff.

All staff are responsible for complying with this policy.

1. SCOPE

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 students. 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 General Data Protection Regulations 2018 (GDPR) which became law on 25th May 2018.

2. DEFINITIONS

Personal data is:	any information about a living person who can be identified (e.g. their name, address, online identifier such as an IP address, academics, school activities, attendance record, discipline, bank details and/or financial information in relations to parents and/or guardians, special education needs, exam results, images of students engaging in school activities, references or expressions of opinion about them). It makes no difference if they can be identified directly from the record itself or indirectly using other information in the School's possession or likely to come into the School's possession. personal information that has been, or will be, word processed or stored electronically (e.g. computer databases and CCTV recordings), personal information that is, or will be, kept in a file which relates to an individual or in a filing system that is organised by reference to criteria which relate to the individuals concerned (e.g. name, school year, school activities).
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 School has additional obligations in connection with the use of sensitive personal data, namely at least one of the following conditions must be satisfied: • Explicit consent of the data subject must be obtained • Necessary for carrying out the obligations under employment, social security or social protection law or a collective agreement • Used in connection with alumni relations provided it relates solely to this and there is no disclosure to a third party without consent • Data manifestly made public by the data subject • Various public interest situations as outlined in the General Data Protection Regulations 2018
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 students.
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.
The Information Security Officer:	The School has appointed the Business and Facilities Manager as its Information Security Officer, responsible for day to day compliance with this Policy.

3. ACQUIRING USING AND DISPOSAL OF PERSONAL DATA

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

- providing students 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 students 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.
- providing an education, training and pastoral care.
- providing activities for students and parents - this includes school trips and activity clubs.
- providing academic, examination and career references for students and staff.
- protecting and promoting the interests and objectives of the School - this includes fundraising.
- safeguarding and promoting the welfare of students.
- monitoring students' and staff's email communications, internet and telephone use to ensure students and staff are following the School's IT Acceptable Use policy.
- promoting the School to prospective students and their parents.
- communicating with former students.
- for personnel, administrative and management purposes. For example, to pay staff and to monitor their performance.
- fulfilling the School's contractual and other legal obligations.

3.2 Staff should seek advice from the Information Security 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 Information Security Officer's permission.

3.3 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.

3.4 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 GDPR will be adequately protected and the transfer has been approved by the Information Security Officer. This applies even if the transfer is to a pupil's parents or guardians living outside the EEA.

3.5 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 GDPR.

3.6 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 and Data Retention Policy. Staff should not delete records containing personal data without authorisation.

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

4. INFORMATION AND EXPLANATION

Privacy Notices: 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 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/.

Staff are not expected to routinely provide students, 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 and School Workforce can be obtained from the Information Security Officer or accessed on the School's website.

Use: Having said this, staff should inform the Information Security 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 information about students without telling their parents what that information will be used for.

5. PROTECTING CONFIDENTIALITY

5.1 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: the School Nurse may disclose details of a cleaning lady's allergy to bee stings to colleagues so that they will know how to respond, but more private health matters must be kept confidential;

- 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, students or other members of staff unless the member of staff has given their permission.

5.2 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 GDPR. However, staff should always speak to the Information Security Officer if in doubt, or if staff are being asked to share personal data in a new way.

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

- make sure they are allowed to share it – that they have the necessary consent;
- 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
- 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 GDPR as well. Specific guidance on this is provided in the School's Images Policy available on the School's website.

5.4 Information security and protecting personal data: Information security is the most important aspect of data protection compliance and most of the fines under the GDPR 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:

- paper records which include confidential information shall be kept in a cabinet or office which is kept locked when unattended.
- 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.
- 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 Head of IT Services.
- 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.

6. DATA BREACHES

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

6.1 Reporting obligations: Any actual data breach or alleged data breach must be reported to the Information Security 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. Reference Appendix 1 Data Protection Breach Record

As soon as the School becomes aware of a significant data breach as determined by the Information Security 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:

- mistakenly sending an email containing personal data to an incorrect recipient.
- theft of IT equipment containing personal data.
- 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 Information Security Officer.

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

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. Reference Appendix 2: Subject Access Request Form

7.1 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 Information Security Officer.

7.2 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 Information Security 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. The School has only 30 days' to respond to a Subject Access Request from whenever the request is received.

7.3 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.

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

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

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

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

7.8 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.

7.9 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/.

8. PRIVACY IMPACT ASSESSMENTS

Only really needed where there is a high risk of data getting lost and for all new uses of personal data. As part of schools due diligence in preparing for GDPR we have assessed the use of personal data in school Reference Data Sharing Policy Appendix 1. Privacy Impact Assessments will be completed by the school Information Security Officer and used as part of the schools Auditing Processes. Reference Appendix 3 – Privacy Impact Assessment

9. BREACH OF THIS POLICY

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.

10. COMPLAINTS

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.
Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/.
- Call 0303 123 1113 • Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

11. STATUS

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.

12. RELATED POLICIES

Data Sharing Policy	August 2019 – Version 1.1
Freedom of Information Policy	August 2019 – Version 1.1
Document and Data Retention Policy	August 2019 – Version 1.1
Privacy Notice for Pupils and Parents	August 2019 – Version 1.1
Privacy Notices for School Workforce	August 2019 – Version 1.1
Safe use of Internet and E-Safety Policy	August 2019 – Version 2.1
School Workforce Acceptable use of ICT Policy	August 2019 – Version 1.1

13. FURTHER INFORMATION

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

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 this website also contains further information about data protection.

Appendix 1: Data Protection Breach Record

Data Protection Breach Record						
Date		**Person responsible for dealing with breach**				
Outline of breach						
Which data subjects are involved						
Reported by						
Phone/email sent to DPO	Y/N	**Is this high risk**	Y/N	**Report to ICO**	Y/N	
Date reported to data subjects						
Actions Taken						
Notes						
Actions approved by:		**Date:**				

Appendix 2: Subject Access Request Form

Subject Access Form	
Name of data subject:	
Name of person who made request:	
Date request received:	
Contact DPO:	John Walker john@jawalker.co.uk 0333 772 9763 or 07736669961
Date acknowledgement sent:	
Name of person dealing with request:	
Notes:	
Are they entitled to the data?	If no reply stating reasons and /or ask for proof
Do you understand what data they are asking for?	If no, ask requestor for clarity
Identify the data	What data sources, where are they kept
Do you own the data?	If no, ask third parties to release external data. If data is supplied by another such as Psychology services/Speech and Language service, you do not own the data
Do you need to exempt/redact data?	If exempting/redacting be clear of your reasons Document name, redaction date, why
Is the data going to be ready in time?	Record delays and reasons Communicate with requestor reasons for delays, asking if they would like the data you have collected so far
Create pack	Make sure the data is in an format easy to access, paper, word, excel etc
Inform requestor you have the data	Ask them how they would like it to be delivered
Deliver data	Ask for confirmation/special delivery?
Date Request completed (within 30 days)	
Signed off by:	
At all stages DPO will eb able to provide advice and guidance	

Appendix 3: Privacy Impact Assessment

Privacy Impact Assessment	
What is the aim of the project:	
What data will be collected:	
How will the data be collected?	
Where will the data be stored?	
How will the data to shared?	
How will the data be amended or deleted?	
Identified risks (issues, Risks to individuals, Compliance Risk, School Risk, Possible Solutions)	
Date :	
Signed off by:	