DATA PROTECTION POLICY

MIDDLEWICH HIGH SCHOOL

Updated July 2020

Document Control Information	
Document ID	**MHSDATAPROTECTION01**
Document title	**MHS Data Protection Policy**
Version	**1.1.1**
Status	**APPROVED**
Author	**Rebecca Dale**
Publication date	**25/06/2018**
Next review date	**Every 12 months**

Version History			
Version	**Date**	**Detail**	**Author**
1.0	**11/05/2020**	**Initial**	**Rebecca Dale (RDA)**
1.1	**06/07/2020**	**Updated**	**Rebecca Dale (RDA)**
1.1.1	**13/07/2020**	**Updated**	**Rebecca Dale (RDA)**

Approvals	
Approver	**Date**
Governing Body	**25/06/2018**
Governing Body	**13/07/2020**

Responsibility for updating this policy: Data Protection Lead (DPL)

1. INTRODUCTION

1.1 Middlewich High School is required to process personal data regarding staff, pupils and their parents and guardians and friends of Middlewich High 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.

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- Middlewich High School Standards and Framework Act 1998

1.2. This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- All Article 29/European Data Protection Board Working Party Guidance on the implementation of GDPR
- Department of Education 'Data Protection: a toolkit for schools'
- IRMS Information Management Toolkit for Schools.

1.3. This policy will be implemented in conjunction with the following other school policies:

- Records Management and Retention Policy
- IT Acceptable Use Policy
- CCTV Policy

1.4 All staff are responsible for complying with this policy.

2 SCOPE

This Policy covers Middlewich High 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/Trustees and contractors. It explains

Middlewich High 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 Middlewich High School complies with the Data Protection Act 1998 (the Act) and anticipates the General Data Protection Regulations 2018 (GDPR) which becomes law on 25th May 2018.

3 **Applicable Data**

3.1 Personal data is:

3.1.1 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 pupils 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 Middlewich High School's possession or likely to come into Middlewich High School's possession.

3.1.2 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, year group, School activities).

3.2 Sensitive personal data is:

3.2.1 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.

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

3.2.2 Explicit consent of the data subject must be obtained
3.2.3 Necessary for carrying out the obligations under employment, social security or social protection law or a collective agreement
3.2.4 Used in connection with alumni relations provided it relates solely to this and there is no disclosure to a third party without consent
3.2.5 Data manifestly made public by the data subject
3.2.6 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:

Middlewich High 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 Middlewich High School is responsible for complying with the Act.

3.5 The Data Protection Officer:

3.5.1. Middlewich High School has appointed a DPO in order to:

- Inform and advise Middlewich High School and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor Middlewich High School compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

3.5.2 The role of DPO will be carried out by an experienced and qualified member of staff as designated by Cheshire West and Chester Council.

3.5.3. Middlewich High School will make freely available the contact details for their appointed DPO:
Schools Data Protection Officer
Cheshire West and Chester Council,
3rd Floor,
Civic Way,
4 Civic Way,
Ellesmere Port,
CH65 0BE
Email: schoolDPO@cheshirewestandchester.gov.uk

3.5.4. The DPO will operate independently, their role being to:

- Advise Middlewich High School and its employees about the obligations to comply with GDPR and other data protection requirements – this could be to assist in implementing a new CCTV system or to respond to questions or complaints about information rights.
- Monitor Middlewich High School's compliance with GDPR, advising on internal data protection activities such as training for staff, the need for data protection impact assessments and conducting internal audits.
- Act as the first point of contact with the Information Commissioner's Office and for individuals whose data Middlewich High School processes.

3.5.5. Where advice and guidance offered by the DPO is rejected by Middlewich High School, this will be independently recorded.

3.5.6 Advice offered by the DPO will only be declined at the direction of the Head and/or Governing body and will be provided to the DPO in writing.

3.5.7 Ms. Rebecca Dale as its Data Protection Lead, responsible for day-to-day compliance with this Policy. She can be contacted at Middlewich High School, King Edward Street, Middlewich, Cheshire CW10 9BU, by telephone on 01606 288170 or at rdale@middlewichhigh.cheshire.sch.uk

4.0 ACQUIRING, USING AND DISPOSAL OF PERSONAL DATA

4.1 Middlewich High School shall only process personal data for specific and legitimate purposes. These are:

- providing pupils and staff with a safe and secure environment including images on CCTV – all cameras around Middlewich High 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 28 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 pupils and parents - this includes School trips and activity clubs
- providing academic, examination and career references for pupils and staff
- protecting and promoting the interests and objectives of Middlewich High School - this includes fundraising
- safeguarding and promoting the welfare of pupils
- monitoring pupils' and staff's email communications, internet and telephone use to ensure pupils and staff are following Middlewich High School's Computer Security Policy
- promoting Middlewich High School to prospective pupils and their parents
- communicating with former pupils
- for personnel, administrative and management purposes. For example, to pay staff and to monitor their performance
- fulfilling Middlewich High School's contractual and other legal obligations

4.1.1 Middlewich High School will ensure that, where it processes personal data it will be lawfully processed under one of the following conditions:

- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For the performance of a contract with the data subject or to take steps to enter into a contract.

- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

4.1.2. In addition, Middlewich High School will ensure that the processing of sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Protecting the vital interests of a data subject or another individual here the data subject is physically or legally incapable of giving consent.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims
- Processing is necessary for reasons of substantial public interest, on the basis of Union or Member state law, with full regard for the rights and interests of the data subject.
- Processing is necessary for the purposes of preventive or occupational medicine, for example, the assessment of the working capacity of the employee
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

4.2 Staff should seek advice from the Data Protection Lead 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 Middlewich High School shall not hold unnecessary personal data, but shall hold sufficient information for the purpose for which it is required. Middlewich High 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 Middlewich High School shall not transfer personal data outside the European Economic Area (EEA) without the data subject's permission. This applies even if the transfer is to a pupil's parents or guardians living outside the EEA**.**

4.5 When Middlewich High School acquires personal information that will be kept as personal data, Middlewich High 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.

4.6 Middlewich High 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 Middlewich High School's Record Management Policy. Staff should not delete records containing personal data without authorisation.

4.7 Middlewich High School will keep personal data secure and adopt technical and organisational measures to prevent unauthorised or unlawful processing of personal data

4.8 In accordance with the requirements outlined in the GDPR, personal data will be:

1. Processed Fairly, Lawfully and Transparently
2. Processed for a Specified and Legitimate Purpose
3. Adequate, Relevant and limited to what is relevant
4. Accurate and up to date
5. Kept no longer than necessary
6. Stored securely using technical and organisational measures

The GDPR also requires that "the controller (Middlewich High School) shall be responsible for, and able to demonstrate, compliance with the principles".

5.0 ACCOUNTABILITY

5.1. Middlewich High School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR. This can take a variety of forms. Examples of technical and organisational measures can be found below.

Technical Measures

- Firewalls
- Anti-virus software
- Encryption
- Secure emails
- VPNs (Virtual Private Networks)

Organisational Measures

- Policies and Procedures in place to help staff understand their duties under data protection
- Training
- A more knowledgeable and open culture towards Data Protection

5.2. Middlewich High School will provide comprehensive, clear and transparent privacy notices.
5.3. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data.
5.4. In line with best practice, we shall maintain a record of processing activities will include as a minimum the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules

- Categories of recipients of personal data
- Description of technical and organisational security measures

5.5. Middlewich High School will implement measures that meet the principles of data protection, continuously creating and improving security features.

5.6. Middlewich High School will produce Data Protection Impact Assessments where the processing of personal data is likely to result in a high risk to the rights of the individual, where a major project requires the processing of personal data or before the introduction of new technology or a significant change to the way processing is performed.

6.0 INFORMATION AND EXPLANATION

6.1 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.

6.2 Purpose: The privacy notice is to ensure that Middlewich High 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/.

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

6.4 Use: Having said this, staff should inform the Data Protection Officer if they suspect that Middlewich High 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 Middlewich High School is collecting medical information about pupils without telling their parents what that information will be used for

7.0 LAWFUL PROCESSING

7.1. The legal basis for processing data will be identified and documented prior to data being processed. The school will make it clear, at all times, the basis on which personal data is processed.

7.2. Middlewich High School will ensure that, where it processes personal data it will be lawfully processed under one of the following conditions:
- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

7.3. In addition, Middlewich High School will ensure that the processing of sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Protecting the vital interests of a data subject or another individual here the data subject is physically or legally incapable of giving consent.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims
- Processing is necessary for reasons of substantial public interest, on the basis of Union or Member state law, with full regard for the rights and interests of the data subject.
- Processing is necessary for the purposes of preventive or occupational medicine, for example, t the assessment of the working capacity of the employee
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

8.0 PROTECTING CONFIDENTIALITY & DATA SECURITY

8.1 Disclosing personal data within Middlewich High 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 Middlewich High School or their relationship to the data subject, unless they need to know it for a legitimate purpose. Examples include: Middlewich High 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 or pupils. It may only be shared with or other members of staff if the member of staff has given their permission

8.2 Disclosing personal data outside of Middlewich High 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 Data Protection Lead if in doubt, or if staff are being asked to share personal data in a new way.

8.3 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

8.4 Confidential paper records will not be left unattended or in clear view anywhere with general access.

8.5 Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

8.6 Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

8.7 Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

8.8 All electronic devices are password-protected to protect the information on the device in case of theft.

8.9 Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

8.10 Staff and governors will not use their personal laptops or computers for school purposes.

8.11 All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

8.12 Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

8.13 Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

8.14 When sending confidential information by fax, staff will always check that the recipient is correct before sending.

8.15 Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

8.16 Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

8.17 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

8.18 The physical security of the school's buildings and storage systems, and access to them, is reviewed on an annual basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

8.19 Any unauthorised disclosure or personal or sensitive information may result in disciplinary action.

9.0 Consent

9.1. Where there is no other legal basis for the processing of data THE SCHOOL may rely on the consent of individuals, both parents and pupils, in seeking consent.

9.2. Where used, consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

9.3. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

9.4 Where consent is given, a record will be kept documenting how and when consent was given.

9.5 Consent can be withdrawn by the individual at any time.

9.6 The consent of parents will be sought prior to the processing of a child's data under the age of 12 except where the processing is related to preventative or counselling services offered directly to a child.

10. The right to be informed

10.1 The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

10.2 If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

10.3 In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and where applicable, the controller's representative and the DPO.
- The purpose of, and the legal basis for, processing the data.
- Any legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.

10.4 Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

11. The right of access

11.1 Individuals have the right to obtain confirmation that their data is being processed.

11.2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. A form for requesting information is available from the school website.

11.3 Middlewich High School will verify the identity of the person making the request before any information is supplied as well as confirming the subject of the request and the right to make such a request (see 11.12. and 11.13)

11.4 A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

11.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

11.6 Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee may be charged.

11.7 All fees will be based on the administrative cost of providing the information.

11.8 All requests will be responded to without delay and at the latest, within one month of receipt. Where a requests is received and identify confirmed, the request will be responded to by the corresponding date in the next month.

11.9 In the event of numerous or complex requests, the period of compliance may be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

11.10 Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

11.11 In the event that a large quantity of information is being processed about an individual, the school may ask the individual to specify the information the request is in relation to.

11.12 A parent or guardian does not have an automatic right to information held about their child. The right belongs to the child and the parent(s) acts on their behalf, where they have parental responsibility for the child. In England the age at which a child reaches sufficient maturity to exercise their own right to access their information is normally 12, but this may vary amongst individuals. Once a child reaches sufficient maturity, the parent may only act with their child's consent.

11.13 Where a child is over 12 and a request is made on their behalf, the school may contact them separately to seek their signed consent for someone to access their records on their behalf. When deciding whether information about a child can be released, consideration will be given to the best interests of the child.

11.14 The school will clearly communicate and promote the process for the submission of Subject Access Requests and the exercising of other individual rights as defined under the GDPR during holiday periods, stating clearly how the school will handle these requests.

12. The right to rectification

12.1 Individuals are entitled to have any inaccurate or incomplete personal data rectified.

12.2 Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

12.3 Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

12.4 Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex and where it is agreed with the Data Protection Officer.

12.5 Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

13. The right to erasure

13.1 Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

13.2 The right to erasure is not absolute. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation

13.3 Middlewich High School has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

13.4 As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

13.5 Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

13.6 Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question where possible.

14. The right to restrict processing

14.1 Individuals have the right to block or suppress the school's processing of personal data in certain circumstances.

14.2 In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

14.3 Middlewich High School will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual

- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

14.4 If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

14.5 The school will inform individuals when a restriction on processing has been lifted.

15. The right to data portability

15.1 Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

15.2 Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

15.3 The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a the school
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

15.4 Personal data will be provided in a structured, commonly used and machine-readable form.

15.5 Middlewich High School will provide the information free of charge.

15.6 Where feasible, data will be transmitted directly to another organisation at the request of the individual.

15.7 Middlewich High School is not obligated to adopt or maintain processing systems which are technically compatible with other organisations.

15.8 In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

15.9 Middlewich High School will respond to any requests for portability within one month.

15.10 Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

15.11 Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

16. The right to object

16.1 Middlewich High School will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

16.2 Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing undertaken by or on behalf of the school
- Processing for purposes of scientific or historical research and statistics.

16.3 Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

16.4 Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

16.5 Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

16.6 Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

17. Privacy by design and Data Protection Impact Assessments

17.1 Middlewich High School will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

17.2 Data Protection Impact Assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

17.3 DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation, which might otherwise occur.

17.4 A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

17.5 A DPIA may be used for more than one project, where necessary and where the aims and conditions of the project are the same.

17.6 Middlewich High School will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

17.7 Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

18. Data Processors

18.1 Middlewich High School will ensure that whenever it employs or utilises a data processor a written contract will be in place.

18.2 Any contract will include, as a minimum, specific terms under which processing is allowed and will document:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

18.3 Where appropriate, and if and when supplied by the Information Commissioner's Office, standard clauses may be supplemented.

18.4 Any contract will clearly identify the responsibilities and liabilities of data processors in relation to:

- not to use a sub-processor without the prior written authorisation of the data controller;
- to co-operate with supervisory authorities (such as the ICO);
- to ensure the security of its processing;
- to keep records of processing activities;
- to notify any personal data breaches to the data controller;
- to employ a data protection officer; and
- to appoint (in writing) a representative within the European Union if needed.

18.5 Where a processor fails in these obligations or acts outside of the direct instructions of the school, appropriate action will be taken.

19.0 DATA BREACHES

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

19.2 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 Middlewich High 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

19.3 Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required to do so will be a breach of school policy and an additional breach of the GDPR.

20. CCTV

20.1. Middlewich High School operates CCTV on the premises and is mindful of the GDPR implications of this. A separate CCTV policy is held by the school and is available for inspection on the school website.

20.2 Requests for access to CCTV are covered in both the CCTV policy, for general requests, and the Information Rights Policy, for Subject Access Requests.

21.0 Biometric Data

21.1 Schools that use pupils' biometric data must treat the data collected with appropriate care and must comply with the data protection principles as set out in the General Data Protection Regulations (GDPR) 2018.

21.2 Where the data is to be used as part of an automated biometric recognition system, schools and colleges must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.

21.2 Middlewich High School must ensure that each parent of a child is notified of the School's intention to use the child's biometric data as part of an automated biometric recognition system.

21.3 The written consent of at least one parent must be obtained before the data is taken from the child and used i.e., 'processed'. This applies to all pupils in schools and colleges under the age of 18. In no circumstances can a child's biometric data be processed without written consent.

21.4 The schools must not process the biometric data of a pupil (under 18 years of age) where:
a) The child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data
b) No parent has consented in writing to the processing
c) A parent has objected in writing to such processing, even if another parent has given written consent

21.5 The school must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system. 1.

21.6 What is biometric data?

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data.

21.6.1 The Information Commissioner considers all biometric information to be sensitive personal data as defined by the GDPR 2018; this means that it must be obtained, used and stored in accordance with that Regulation.

21.6.2 The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the GDPR 2018.

21.7 What is an automated biometric recognition system?

An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

21.7.2 Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in 21.6 above.

21.8 What does processing data mean?

'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it.

21.8.1 An automated biometric recognition system processes data when:

a) Recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner

b) Storing pupils' biometric information on a database system

c) Using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.

21.9 Frequently Asked Questions

21.9.1 What information should schools provide to parents/pupils to help them decide whether to object or for parents to give their consent?

Any objection or consent by a parent must be an informed decision – as should any objection on the part of a child. Schools should take steps to ensure parents receive full information about the processing of their child's biometric data including a description of the kind of system they plan to use, the nature of the data they process, the purpose of the processing and how the data will be obtained and used. Children should be provided with information in a manner that is appropriate to their age and understanding.

21.9.2 What if one parent disagrees with the other?

The schools will be required to notify each parent of a child whose biometric information they wish to collect/use. If one parent objects in writing, then the school or college will not be permitted to take or use that child's biometric data.

21.9.3 How will the child's right to object work in practice – must they do so in writing?

A child is not required to object in writing. An older child may be more able to say that they object to the processing of their biometric data. A younger child may show reluctance to take part in the physical process of giving the data in other ways. In either case the school or college will not be permitted to collect or process the data.

21.9.4 Are schools required to ask/tell parents before introducing an automated biometric recognition system?

Schools are not required by law to consult parents before installing an automated biometric recognition system. However, they are required to notify parents and secure consent from at least one parent before biometric data is obtained or used for the purposes of such a

system. It is up to schools to consider whether it is appropriate to consult parents and pupils in advance of introducing such a system.

21.9.5 Do schools need to renew consent every year?

No. The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time if another parent or the child objects to the processing (subject to the parent's objection being in writing). When the pupil leaves the school, their biometric data should be securely removed from the school's biometric recognition system.

21.9.6 Do schools need to notify and obtain consent when the school introduces an additional, different type of automated biometric recognition system?

Yes, consent must be informed consent. If, for example, a school has obtained consent for a fingerprint/fingertip system for catering services and then later introduces a system for accessing library services using iris or retina scanning, then schools will have to meet the notification and consent requirements for the new system.

21.9.7 Can consent be withdrawn by a parent?
Parents will be able to withdraw their consent, in writing, at any time. In addition, either parent will be able to object to the processing at any time but they must do so in writing.

21.9.8 When and how can a child object?

A child can object to the processing of their biometric data or refuse to take part at any stage – i.e. before the processing takes place or at any point after his or her biometric data has been obtained and is being used as part of a biometric recognition system. If a pupil objects, the school or college must not start to process his or her biometric data or, if they are already doing this, must stop. The child does not have to object in writing.

21.9.9 Will consent given on entry to secondary school be valid until the child leaves that school?

Yes. Consent will be valid until the child leaves the school – subject to any subsequent objection to the processing of the biometric data by the child or a written objection from a parent. If any such objection is made, the biometric data should not be processed and the school must, in accordance with the GDPR, remove it from the school's system by secure deletion.

21.9.10 Can the school notify parents and accept consent via email?

Yes – as long as the school is satisfied that the email contact details are accurate and the consent received is genuine.

21.9.11 Will parents be asked for retrospective consent?

No. Any processing that took place prior to the provisions in the Protection of Freedoms Act coming into force will not be affected. Any school wishing to continue to process biometric data must have already sent the necessary notifications to each parent of a child and obtained the written consent from at least one of them before continuing to use their child's biometric data.

21.9.12 Does the legislation cover other technologies such a palm and iris scanning?

Yes. The legislation covers all systems that record or use physical or behavioural characteristics for the purpose of identification. This includes systems that use palm, iris or face recognition, as well as fingerprints.

21.9.13 Is parental notification and consent required under the Protection of Freedoms Act 2012 for the use of photographs and CCTV in schools?

No – not unless the use of photographs and CCTV is for the purposes of an automated biometric recognition system. However, schools must continue to comply with the requirements in the GDPR 2018 when using CCTV for general security purposes or when using photographs of pupils as part of a manual ID system or an automated system that uses barcodes to provide services to pupils. Depending on the activity concerned, consent may be required under the GDPR before personal data is processed.

The Government believes that the GDPR requirements are sufficient to regulate the use of CCTV and photographs for purposes other than automated biometric recognition systems. Photo ID card systems, where a pupil's photo is scanned automatically to provide them with services, would come within the obligations on schools and colleges under sections 26 to 28 of the Protection of Freedoms Act 2012, as such systems fall within the definition in that Act of automated biometric recognition systems.

Please refer to the CCTV Policy for more information.

21.9.14 Is parental notification or consent required if a pupil uses or accesses standard commercial sites or software which use face recognition technology?

The provisions in the Protection of Freedoms Act 2012 only cover processing by or on behalf of a school or college. If a school or college wishes to use such software for school work or any school business, then the requirement to notify parents and to obtain written consent will apply. However, if a pupil is using this software for their own personal purposes then the provisions do not apply, even if the software is accessed using school equipment

22. Data retention

22.1 Data will not be kept for longer than is necessary in line with the schools Record Management Policy.

22.2 Unrequired data will be deleted as soon as practicable.

22.3 Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

22.4 Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

23. DBS data

23.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

23.2 Data provided by the DBS will never be duplicated.

23.3 Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

24.0 BREACH OF THIS POLICY

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

25.0 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.

26.0 FURTHER INFORMATION

26.1 Further information and guidance regarding this policy or its application can be obtained from the school's Data Protection Lead – Mrs Rebecca Dale.