WIMBORNE
Academy Trust

GDPR DATA PROTECTION POLICY

Version	2.0
Approving Body	Trust Board
Date ratified	June 2018
Date issued	June 2018
Review date	September 2019
Owner	Chief Executive Officer
Applies to	All Trust Schools, all Trust staff

Version	**Date**	**Reason**
1.0	September 2015	To establish a Trustwide policy
2.0	June 2018	To replace previous Data Protection Policy following the introduction of GDPR

CONTENTS

STATEMENT OF INTENT

Wimborne Academy Trust ("Trust") is a group of academy schools.

The Trust collects, controls and processes personal information about its staff and pupils and their families.

The Trust shares personal information about its staff and pupils and their families with third-party organisations in certain circumstances.

The Trust will only control, process and share personal information where it has a lawful basis to do so under the General Data Protection Regulation (GDPR).

The Trust will ensure that staff and pupils and their families are aware that of the circumstances in which their personal information is collected, controlled, processed and shared, and will ensure that they are aware of their rights in relation to this personal information.

This policy is in place to ensure all staff and those involved in the governance of the Trust are aware of their responsibilities, and outlines how the Trust complies with the following core principles of the GDPR.

1. Legal framework

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

- The General Data Protection Regulation
- 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
- The School Standards and Framework Act 1998

1.2. This policy also has regard to the following guidance:

- ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'

2. Applicable data

2.1. For the purpose of this policy, **personal information** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address.

2.2. **Sensitive personal information** is referred to in the GDPR as 'special categories of personal information', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

3. Principles

3.1. In accordance with the requirements outlined in the GDPR, personal information will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; reasonable steps must be taken to ensure that personal information that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information are processed.

- Processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.2. The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4. Accountability

4.1. Wimborne Academy Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

4.2. The Trust will provide comprehensive, clear and transparent privacy policies.

4.3. Internal records of the school's processing activities will be maintained and kept up-to-date.

4.4. The Trust will implement measures that meet the principles of data protection by design and data protection by default.

4.5. Data protection impact assessments will be used, where appropriate.

5. Data protection officer (DPO)

5.1. A DPO will be appointed in order to:

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

5.2. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

5.3. The individual appointed as DPO will have suitable experience and knowledge of data protection law, particularly that in relation to schools.

5.4. The DPO will report to the highest level of management at the Trust, which is the CEO.

5.5. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

5.6. The current DPO for the Trust is Ross Bowell, the policy will be updated as and when the postholder changes.

6. Lawful processing

6.1. The legal basis for processing data will be identified.

6.2. Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained or
- Processing is necessary for:
  - Compliance with a legal obligation or
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or
  - For the performance of a contract with the data subject or to take steps to enter into a contract or
  - Protecting the vital interests of a data subject or another person.

6.3. 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 or
- Processing relates to personal information manifestly made public by the data subject or
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement or
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent or
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity or
  - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards or
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional or
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices or
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with article 89(1).

7. Consent

7.1. Where consent is required, it must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

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

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

7.4. The Trust ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

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

7.7. Where a child is under the age of 16, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

8. The right to be informed

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

8.2. 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 the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal information.
- 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.

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

8.4. Where data is not obtained directly from the data subject, information regarding the categories of personal information that the Trust holds, the source that the personal information originates from and whether it came from publicly accessible sources, will be provided.

9. The right of access

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

9.2. Individuals have the right to submit a **Subject Access Request** (SAR) to gain access to their personal information in order to verify the lawfulness of the processing. Requests must be confirmed in writing, preferably in the form of a letter or email addressed to data.protection@wimborneacademytrust.org

9.3. The Trust will verify the identity of the person making the request before any information is supplied.

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

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

9.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

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

9.8. All requests will be responded to without delay and at the latest, within one month of receipt.

9.9. In the event of numerous or complex requests, the period of compliance will 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.

9.10. Where a request is manifestly unfounded or excessive, the Trust 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.

9.11. In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.

10. The right to rectification

10.1. Individuals are entitled to have any inaccurate or incomplete personal information rectified.

10.2. Where the personal information in question has been disclosed to third parties, the Trust will inform them of the rectification where possible.

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

10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

10.5. Where no action is being taken in response to a request for rectification, the Trust 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.

11. The right to erasure

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

11.2. Individuals have the right to erasure in the following circumstances:

- Where the personal information 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 information was unlawfully processed
- The personal information is required to be erased in order to comply with a legal obligation
- The personal information is processed in relation to the offer of information society services to a child

11.3. The Trust has the right to refuse a request for erasure where the personal information 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

11.4. 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.

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

11.6. Where personal information has been made public within an online environment, the Trust will inform other organisations who process the personal information to erase links to and copies of the personal information in question.

12. The right to restrict processing

12.1. Individuals have the right to block or suppress the Trust processing of personal information.

12.2. In the event that processing is restricted, the Trust will store the personal information, 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.

12.3. The school will restrict the processing of personal information in the following circumstances:

- Where an individual contests the accuracy of the personal information, processing will be restricted until the Trust has verified the accuracy of the data
- Where an individual has objected to the processing and the Trust 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 Trust no longer needs the personal information but the individual requires the data to establish, exercise or defend a legal claim

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

12.5. The Trust will inform individuals when a restriction on processing has been lifted.

13. The right to data portability

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

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

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

- To personal information that an individual has provided to a controller
- 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

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

13.5. The Trust will provide the information free of charge.

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

13.7. The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

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

13.9. The Trust will respond to any requests for portability within one month.

13.10. 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.

13.11. Where no action is being taken in response to a request, the Trust 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.

14. The right to object

14.1. The Trust will inform individuals of their right to object in the privacy notice.

14.2. Individuals have the right to object to the following:

- Processing based on the performance of a task in the public interest
- Direct marketing

- Processing for purposes of scientific or historical research and statistics.

14.3. Where personal information is processed for the performance of a legal task:

- An individual's grounds for objecting must relate to his or her particular situation.
- The Trust will stop processing the individual's personal information unless the processing is for the establishment, exercise or defence of legal claims.

14.4. Where personal information is processed for direct marketing purposes:

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

14.5. Where personal information 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 information is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.

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

15. Automated decision making and profiling

15.1. Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

15.2. The Trust will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

15.3. When automatically processing personal information for profiling purposes, the Trust will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.

- Securing personal information in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

15.4. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The Trust has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

16. Privacy by design and privacy impact assessments

16.1. The Trust will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

16.2. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

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

16.4. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals. A programme of retrospective DPIAs to cover existing technologies will be agreed by the Trust and completed during 2018/19.

16.5. A DPIA will be used for more than one project, where necessary.

16.6. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal information which is in relation to criminal convictions or offences
- The use of CCTV.

16.7. The Trust 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. Data breaches

17.1. The term ‘personal information breach’ refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal information.

17.2. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

17.3. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Trust becoming aware of it.

17.4. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

17.5. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust will notify those concerned directly.

17.6. A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

17.7. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

17.8. Effective and robust breach detection, investigation and internal reporting procedures are in place at the Trust, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

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

- The nature of the personal information 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 information breach
- A description of the proposed measures to be taken to deal with the personal information breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

17.10. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

18. Security of personal information

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

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

18.3. Personal information in digital format will be collected, processed, stored and shared in accordance with the Trust's Data and Network Security Policy

18.4. Where personal information that could be considered private or confidential is taken off the premises, either in digital 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 Trust premises accepts full responsibility for the security of the personal information.

18.5. Before sharing personal information, staff members will ensure:

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

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

18.7. Wimborne Academy Trust takes its duties under GDPR seriously and any unauthorised disclosure may result in disciplinary action.

19. Publication of information

19.1. Wimborne Academy Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

19.2. Classes of information specified in the publication scheme are made available quickly and easily on request.

19.3. Wimborne Academy Trust will not publish any personal information, including photos, on its websites without the permission of the affected individual.

20. CCTV and photography

20.1. The Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

20.2. The Trust notifies all pupils, staff and visitors of the purpose for collecting CCTV images.

20.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

20.4. All CCTV footage will be kept for six months for security purposes; each school's substantive [i]Headteacher is responsible for keeping the records secure and allowing access.

20.5. The Trust will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

20.6. If the Trust wishes to use images/video footage of pupils in a publication, such as a school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

20.7. Precautions are taken when publishing photographs of pupils, in print, video or on the Trust/ schools' websites.

20.8. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

21. Data retention

21.1. Data will not be kept for longer than is necessary.

21.2. Unrequired data will be deleted as soon as practicable.

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

22. DBS data

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

[i] Throughout this policy, Headteacher also refers to Head of School