Data Protection Policy

The Bishop of Winchester Academy

Document Control Table	
Policy Title	**Data Protection Policy**
Author: Name, Code, Role	Moira Lyons-Montgomery, MLM, EA to Principal
Policy Version (V) Nº	2
Statutory	Yes ☑ No ☐ Internal Policy
Policy Required on Website	Yes ☐ No ☑
Policy Approval Date	Approved Full Board 08.07.25
Policy Approval Route	☐ Author – ALT ☑ Author - ALT - Trust Board ☐ Author - ALT - Resources Committee ☐ Author - ALT - Student Experience Committee
Policy Review Frequency	**ALT** annual ☑ biennial ☐ quadrennial ☐ **Trust committee** annual ☐ biennial ☐ quadrennial ☐ **Trust board** annual ☑ biennial ☐ quadrennial ☐ **Other** (state)
Linked Policies (if any)	• FoI Policy • Data Retention Policy • Privacy notices • Safeguarding Policy Note; TBOWA does not process biometric data
Next Review Due by Author and ALT	Following approval above, Pentecost 2026
Next Review Due by Committee	n/a
Next Review Due by Board	Following approval above, Pentecost 2026

History			
V	**Date**	**Author Code**	**Revision Summary**
1			Full board approved: 11 July 2024
2	Pentecost	MLM	Addition of a control table. 'School' changed to 'Academy' throughout. 'The Bishop of Winchester Academy' added where a field was left blank for the insertion of a specific setting. GDPR corrected to UK GDPR and the Data Protection Act. 5.2.1 information added about the incoming Data (Use and Access) bill and the change of ICO to IC.
		DPO	Reviewed by DPO (C. Howard), Satswana, 04.05.25 - meets ICO and DfE requirements. Approved full board 08.07.25
3	Lent	JHU	Change to DPO from Satswana to Global Policing as of 01.02.26

Contents

Sponsors Statement

All The Bishop of Winchester Academy (TBOWA) policies exist to support the Sponsors' vision, Christian ethos and values that are embedded in the day-to-day and long-term running of the academy. Each policy evidences the commitment of the Sponsors to the principles and values of honesty, respect, hospitality, compassion, love, forgiveness, self-discipline, creativity and hope. This policy contributes to the development of young people and the community through all Academy activities.

1 Intent

1.1 Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as an academy trust, we will collect, store and **process personal data** about our pupils, workforce, parents and others. This makes us a **data controller** in relation to that **personal data**.

1.2 We are committed to the protection of all personal data and special category personal data for which we are the data controller.

1.3 The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

1.4 All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

2 Introduction

2.1 The academy is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

2.2 The Academy may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Local Authority, other academies and educational bodies, and potentially social services.

2.3 This policy is in place to ensure all staff and trustees are aware of their responsibilities and outlines how the Academy complies with the following core principles of the UK GDPR and the DPA.

2.4 Organisational methods for keeping data secure are imperative, and TBOWA believes that it is good practice to keep clear practical policies, backed up by written procedures.

3 Who is responsible for carrying out this policy?

3.1 The implementation of this policy will be monitored by the governing body of The Bishop of Winchester Academy and remain under review by the ALT (advanced leadership team). The principal acts as the representative of the data controller on a day-to-day basis.

4 Data Protection Officer

4.1 As a Trust, we are required to appoint a Data Protection Officer ("DPO"). Our DPO is Global Policing Ltd who can be contacted at **data@globalpolicing.co.uk** or 0161 510 2999.

4.2 The ALT is responsible for ensuring compliance with the data protection legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the ALT.

4.3 The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

4.4 The EA to the principal provides day to day data protection advice within the academy and is the point of contact for information between the DPO and the academy.

5 Legal framework

5.1 This policy meets the requirements of the:

5.1.1 UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020.

5.1.2 Data Protection Act 2018 (DPA 2018).

5.1.3 It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

5.2 This policy also has regard to the following guidance:

5.2.1 The Data (Use and Access) bill, which formed the Information Commission.

6 Applicable data

6.1 For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

6.2 Sensitive personal data is referred to in the UK GDPR as 'special categories of personal data', 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.

7 Principles

7.1 In accordance with the requirements outlined in the UK GDPR the Academy will seek to ensure that all personal data will be:

7.1.1 Processed lawfully, fairly and in a transparent manner in relation to individuals.

7.1.2 Collected for specified, explicit and legitimate purposes

7.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

7.1.4 Accurate and, where necessary, kept up-to-date

7.1.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.

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

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

8 Accountability

8.1 The Bishop of Winchester Academy will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.

8.2 The Academy will provide comprehensive, clear and transparent privacy policies.

8.3 Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data (Article 9) or that in relation to criminal convictions and offences (Article 10)

8.4 Internal records of processing activities will include the following:

8.4.1 Name and details of the organisation

8.4.2 Purpose(s) of the processing

8.4.3 Description of the categories of individuals and personal data

8.4.4 Retention schedules

8.4.5 Categories of recipients of personal data

8.4.6 Description of technical and organisational security measures

8.4.7 Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

8.5 The Academy will implement measures that meet the principles of data protection by design and data protection by default, such as:

8.5.1 Data minimisation.

8.5.2 Pseudonymisation.

8.5.3 Transparency.

8.5.4 Allowing individuals to monitor processing.

8.5.5 Continuously creating and improving security features.

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

9 Lawful processing

9.1 The legal basis for processing data will be identified and documented prior to data being processed.

9.2 Under the UK GDPR, data will be lawfully processed under the following conditions:

9.2.1 The consent of the data subject has been obtained.

9.2.2 Processing is necessary for:

(a) Compliance with a legal obligation.

(b) The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

(c) For the performance of a contract with the data subject or to take steps to enter into a contract.

(d) Protecting the vital interests of a data subject or another person.

(e) 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.

9.3 Sensitive data or "Special categories of personal data" will only be processed under the following conditions:

9.3.1 Processing is necessary for:

(a) Carrying out obligations under employment, social security or social protection law, or a collective agreement.

(b) Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.

(c) The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

(d) 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.

(e) 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.

(f) Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

10 Consent

10.1 Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

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

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

10.4 The Academy ensures that consent mechanisms meet the standards of the UK 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.

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

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

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

11 The right to be informed

11.1 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.

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

11.3 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:

11.3.1 The identity and contact details of the controller, and where applicable, the controller's representative and the DPO.

11.3.2 The purpose of, and the legal basis for, processing the data.

11.3.3 The legitimate interests of the controller or third party.

11.3.4 Any recipient or categories of recipients of the personal data.

11.3.5 Details of transfers to third countries and the safeguards in place.

11.3.6 The retention period of criteria used to determine the retention period.

11.3.7 The existence of the data subject's rights, including the right to:

(a) Withdraw consent at any time.

(b) Lodge a complaint with a supervisory authority.

11.4 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.

11.5 Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

11.6 For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

11.7 In relation to data that is not obtained directly from the data subject, this information will be supplied:

11.7.1 Within one month of having obtained the data.

11.7.2 If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

11.7.3 If the data are used to communicate with the individual, at the latest, when the first communication takes place.

12 The right of access

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

12.2 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.

12.3 Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our Academy may not be granted without the express permission of the student. A student's ability to understand their rights will always be assessed on a case-by-case basis.

12.4 The Academy will verify the identity of the person making the request before any information is supplied and may ask the person to provide 2 forms of identification.

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

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

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

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

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

12.10 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.

12.11 Where a request is manifestly unfounded or excessive, the Academy 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.

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

12.13 We may not disclose information for a variety of reasons, such as if it:

12.13.1 Might cause serious harm to the physical or mental health of the pupil or another individual

12.13.2 Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests

12.13.3 Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it

12.13.4 Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

13 The right to rectification

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

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

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

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

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

14 The right to erasure

14.1 Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. This is also known as “the right to be forgotten” under Article 17 of the UK GDPR.

14.2 Individuals have the right to erasure in the following circumstances:

14.2.1 Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed

14.2.2 When the individual withdraws their consent

14.2.3 When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing

14.2.4 The personal data was unlawfully processed

14.2.5 The personal data is required to be erased in order to comply with a legal obligation

14.3 The Academy has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

14.3.1 To exercise the right of freedom of expression and information

14.3.2 To comply with a legal obligation for the performance of a public interest task or exercise of official authority

14.3.3 For public health purposes in the public interest

14.3.4 For archiving purposes in the public interest, scientific research, historical research or statistical purposes

14.3.5 The exercise or defence of legal claims

14.4 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.

14.5 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.

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

14.7 The UK GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

14.7.1 if the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or

14.7.2 if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional).

15 The right to restrict processing

15.1 Individuals have the right to block or suppress the Academy’s processing of personal data.

15.2 In the event that processing is restricted, the Academy 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.

15.3 The Academy will restrict the processing of personal data in the following circumstances:

15.3.1 Where an individual contests the accuracy of the personal data, processing will be restricted until the Academy has verified the accuracy of the data

15.3.2 Where an individual has objected to the processing and the Academy is considering whether their legitimate grounds override those of the individual

15.3.3 Where processing is unlawful and the individual opposes erasure and requests restriction instead

15.3.4 Where the Academy no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

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

15.5 The Academy will inform individuals when a restriction on processing has been lifted.

16 The right to data portability

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

16.2 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.

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

16.3.1 To personal data that an individual has provided to a controller

16.3.2 Where the processing is based on the individual's consent or for the performance of a contract

16.3.3 When processing is carried out by automated means

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

16.5 The Academy will provide the information free of charge.

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

16.7 TBOWA is not required to adopt or maintain processing systems which are technically compatible with other organisations.

16.8 The Academy will respond to any requests for portability within one month.

16.9 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.

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

17 The right to object

17.1 The Academy 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.

17.2 Individuals have the right to object to the following:

17.2.1 Direct marketing

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

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

17.3.1 An individual's grounds for objecting must relate to his or her particular situation.

17.3.2 The Academy will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Academy can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

17.4 Where personal data is processed for direct marketing purposes:

17.4.1 The Academy will stop processing personal data for direct marketing purposes as soon as an objection is received.

17.4.2 The Academy cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

17.5 Where personal data is processed for research purposes:

17.5.1 The individual must have grounds relating to their particular situation in order to exercise their right to object.

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

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

18 Privacy by design and privacy impact assessments

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

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

18.3 DPIAs will allow the Academy to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the reputation of The Bishop of Winchester Academy, which might otherwise occur.

18.4 A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the privacy rights of individuals or compliance risks to the organisation.

18.5 A DPIA will be used for more than one project containing personal data, where necessary.

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

18.6.1 Systematic and extensive processing activities, such as profiling

18.6.2 Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

18.7 The Academy will ensure that all DPIAs include the following information:

18.7.1 A description of the processing operations and the purposes

18.7.2 An assessment of the necessity and proportionality of the processing in relation to the purpose

18.7.3 An outline of the risks to individuals

18.7.4 The measures implemented in order to address risk

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

19 Data breaches

19.1 The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

19.2 The ALT will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

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

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

19.5 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.

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

19.7 A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

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

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

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

19.10.1 The nature of the personal data breach, including the categories and approximate number of individuals and records concerned

19.10.2 The name and contact details of the DPO

19.10.3 An explanation of the likely consequences of the personal data breach

19.10.4 A description of the proposed measures to be taken to deal with the personal data breach

19.10.5 Where appropriate, a description of the measures taken to mitigate any possible adverse effects

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

20 Data security

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

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

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

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

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

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

20.7 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. The person taking the information from the Academy premises accepts full responsibility for the security of the data.

20.8 Before sharing data, all staff members will ensure:

20.8.1 They are allowed to share it.

20.8.2 That adequate security is in place to protect it.

20.8.3 Who will receive the data has been outlined in a privacy notice.

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

20.10 The physical security of the Academy's buildings and storage systems, and access to them, is reviewed as required and no less than on an annual basis.

20.11 If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

20.12 The Bishop of Winchester Academy takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

20.13 The TBOWA appointed Data Protection Officer is Global Policing Ltd

20.14 The IT Manager is responsible for ensuring that continuity and recovery measures are in place locally to ensure the security of protected data.

21 Publication of information

21.1 TBOWA will not publish any personal information, including photos, on its website without the permission of the affected individual.

22 CCTV

22.1 CCTV will be used for monitoring day to day activity in case of criminal activity and to keep people and property safe. Footage will only be accessed should the need arise to investigate any such activity or should we be

requested to access the footage by law. An electronic access log will be kept in relation to requests, footage viewed and who has been identified. This is in line with the ICO's Code of Practice for the use of surveillance cameras and personal information.

23 Artificial intelligence (AI)

23.1 Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The Bishop of Winchester Academy recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

23.2 To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

23.3 If personal and/or sensitive data is entered into an unauthorised generative AI tool, The Bishop of Winchester Academy will treat this as a data breach and will follow the personal data breach procedure outlined in appendix 2.

24 Data retention

24.1 Data will not be kept for longer than is necessary in line with the Academy's Retention Policy.

24.2 Unrequired data will be deleted as soon as practicable.

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

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

25 DBS data

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

25.2 Data provided by the DBS will be handled in accordance with the Retention Policy

25.3 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.

26 Implementation

26.1 This policy will be actively promoted and implemented throughout the Academy.

27 Changes to this policy

We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

Appendix 1

DEFINITIONS

Term	Definition
Biometric Data	is information about a person's physical or behavioural characteristics or features that can be used to identify them and is obtained or recorded for the purposes of a biometric recognition system and can include fingerprints, hand shapes, features of the eye or information about a person's voice or handwriting
Biometric Recognition System	is a system that operates automatically (electronically) and : • Obtains or records information about a person's physical or behavioural characteristics or features; and • Compares or otherwise processes that information with stored information in order to establish or verify the identity of the person or otherwise determine whether they are recognised by the system
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our workforce (including Trustees and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or Biometric Data
Workforce	Includes, any individual employed by Trust such as staff and those who volunteer in any capacity including Trustees / Members/ parent helpers

Appendix 2

Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO). (see 5.2.1)

- On finding or causing a breach or potential breach, the staff member, trustee or data processor must immediately notify the data protection officer (DPO), Global Policing Ltd, by contacting them at **data@globalpolicing.co.uk** or 0161 510 2999.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff and trustees will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Principal who will advise the chair of trustees
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the Academy's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the Academy's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the Academy is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO

- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- The DPO and Principal will review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and Principal will assess recorded data breaches and identify any trends or patterns requiring action by the Academy to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of sensitive data being disclosed via email.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the Academy's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the academy should inform any, or all, of its 3 local safeguarding partners

We will review the effectiveness of these actions and amend them as necessary after any data breach.