The Bishops' Blue Coat Church of England High School

GENERAL DATA PROTECTION REGULATION

DATA PROTECTION POLICY

All of the policies that shape our lives and daily practice at Bishops' are informed by our Christian vision and values to know, nurture and inspire our students to be the best version of themselves so that they can live 'life in all its fullness' (Jn 10:10)

Procedure Name	Data Protection Policy
IS the Policy Statutory?	Yes
SLT member responsible for Code of Practice	Alison Beasley, Business Manager
Author	Alison Beasley, Business Manager and Jonathan Price, Data & Systems Manager
Approved	
Review frequency	2 years

Contents

1. Legal framework 3
2. Applicable data 3
3. Principles 4
4. Accountability 4
5. Data protection officer (DPO) 5
6. Lawful processing 6
7. Consent 7
8. The right to be informed 7
9. The right of access 8
10. The right to rectification 9
11. The right to erasure 9
12. The right to restrict processing 10
13. The right to data portability 10
14. The right to object 11
15. Automated decision making and profiling 12
16. Data Protection by design and default and Data Protection Impact Assessments 12
17. Data breaches 13
18. Data security 14
19. Notification and consent - Biometric data 15
20. Alternative arrangements 17
21. Safeguarding 17
22. Publication of information 18
23. CCTV 18
24 Cloud computing 18
25. Data retention 19
26. DBS data 19
27. Photographs and moving images 19
28. Monitoring 19
Appendix 1 - CCTV Code of Practice 20

Forms available from the school office:

- Data Breach report form
- Biometric consent form

1. Legal framework

1.1. 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
- Protection of Freedoms Act 2012
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- DfE (2023) 'Keeping children safe in education 2023'

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

- Information Commissioner's Office (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- Department of Education (2023) 'Data Protection in school;

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

- Records Management and Retention Plan
- ICT Acceptable Use Policy for students
- ICT Acceptable use policy for staff, governors and volunteers
- Freedom of Information Publication Scheme
- Staff Code of Conduct
- Security Policy
- CCTV code of practice
- Cyber security policy
- Safeguarding policy

2. Applicable data

For the purpose of this policy from here after **The Bishops Blue Coat Church of England High School** is known as "**the school**"

2.1. Personal data refers to information that relates to an identified or identifiable, living individual (Data Subject), including 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.

2.2. Sensitive personal data is defined in the GDPR as 'special categories of personal data', which includes the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, principals, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

2.3. Biometric data**:** Personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, and hand measurements.

2.4. Processing Data is referred to throughout the GDPR and data protection legislation. This means any use of the personal information. This includes collecting, disclosing, destroying, archiving and organising.

2.5. Data Subject is the person who the personal data is about. For example, the children named on a class register at a school are all data subjects of that register.

2.6. Data Controller is usually an organisation who dictates the reason and purpose for how data is processed. The Bishops' Blue Coat Church of England High School (hereafter referred to as 'the school') itself is a Data Controller as it chooses how it collects, uses and shares its own data.

2.7. The Information Commissioner's Office (ICO) is the regulator for Data Protection and Privacy law in the UK. They have the power to enforce on organisations for breaches of the Data Protection Act or the GDPR. This means they can issue: -

- An Undertaking which commits an organisation to improving their Data Protection practices.
- An Enforcement Notice ordering that an organisation does something specific e.g. train all staff to a high standard.
- A Monetary Penalty for serious and significant breaches. Under the General Data Protection Regulation this can be up to €20 Million or 4% of a company's global turnover.

2.8. This policy applies to both automated personal data and to manual filing systems.

3. Principles

3.1. 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

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

4. Accountability

4.1. The 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

4.2. The school will provide comprehensive, clear and transparent privacy notices. The school's Privacy Statements set out in detail how the school will maintain the security of school users' data. The Acceptable Use Policies set out the duties of the staff and other school users in supporting data security.

4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data.

4.4. In line with best practice, the school shall maintain a record of processing activities which 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

4.5. The school will implement measures that meet the principles of data protection, continuously creating and improving security features.

4.6. The 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.

4.7. Within school the security of physical data is coordinated by the school's **Administration and Personnel Manager**

4.8. Within school the security of electronic data is coordinated by the school's **Data and Systems Manager**

4.9 Within school, there is a data protection team consisting of the Business Manager, the Administration and Personnel Manager and the Data and Systems Manager who are responsible for ensuring staff data protection training is kept up to date, and for managing data breaches and requests for information under this policy.

4.9. The governor with special responsibility for data security is **Alex Taylor**

5. Data protection officer (DPO)

5.1. The school has appointed a DPO in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the school's 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.

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.

5.3. The school will make freely available the contact details for their appointed DPO:

Schools Data Protection Officer
Cheshire West and Chester Council,
The Portal,
Wellington Road

Ellesmere Port, CH65 0BA

Email: schoolDPO@cheshirewestandchester.gov.uk

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

- advise the 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 the 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 the school processes.

5.5. Where advice and guidance offered by the DPO is rejected by the school, this will be independently recorded.

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.

6. Lawful processing

6.1. 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.

6.2. The 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.

6.3. In addition, the 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 where 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
- There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted and a decision made only after seeking further clarification.
- Where the school relies on:
- · 'Performance of contract' to process a child's data, the school considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- · 'Legitimate interests' to process a child's data, the school takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.
- · Consent to process a child's data, the school ensures that the requirements outlined in the 'Consent' section are met, and the school does not exploit any imbalance of power in the relationship between the school and the child

7. Consent

7.1. 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.

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

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

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

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

7.6. The consent of parents will be sought prior to the processing of a child's data under the age of 13 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 regard to the processing of their personal data will be written in clear, plain language, which is concise, transparent, easily accessible and free of charge.

8.2. 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.

8.3. 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.

8.4. 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.

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 data in order to verify the lawfulness of the processing.

9.3. The 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 9.12. and 9.13)

9.4. 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.

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 may 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. Where a request is received and identify confirmed, the request will be responded to by the corresponding date in the next month.

9.9. 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.

9.10. 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.

9.11. 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. The time limit for responding to the request will be paused until clarification from the individual is received.

9.12. 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 13, but this may vary amongst individuals. Once a child reaches sufficient maturity, the parent may only act with their child's consent.

9.13. Where a child is over 13 and a request is made on their behalf, the school will seek their consent and contact them separately for 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.

9.14 The school will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data, the school will:

· Omit certain elements from the response if another individual's personal data would be disclosed otherwise.

· Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents or it is reasonable to comply without consent.

· Explain to the individual who made the SAR why their request could not be responded to in full.

10. The right to rectification

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

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

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

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 and where it is agreed with the Data Protection Officer.

10.5. 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.

11. The right to erasure

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

11.2. 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

11.3. The 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

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 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.

11.6. 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.

12. The right to restrict processing

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

12.2. 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.

12.3. The 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

12.4. 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.

12.5. The school 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 data for their own purposes across different services.

13.2. 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.

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

- To personal data that an individual has provided to 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

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

13.5. The school 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 school is not obligated to adopt or maintain processing systems which are technically compatible with other organisations.

13.8. 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.

13.9. The school 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 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.

14. The right to object

14.1. The 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.

14.2. 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.

14.3. 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.

14.4. 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.

14.5. 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.

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

15. Automated decision making and profiling

15.1 The school will only ever conduct solely automated decision making with legal or similarly significant effects is the decision is:

- Necessary for entering into or performance of a contract.
- Authorised by law.
- Based on the individual's explicit consent.

15.2 Automated decisions will not concern a child nor use special category personal data, unless:

- The school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest.

15.3 The school will conduct a DPIA for automated decision making to mitigate risk of errors, bias and discrimination.

15.4 The school will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.

15.5 Individuals have the right not to be subject to a decision when both of the following conditions are met:

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

15.6 The school 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.

15.7 When automatically processing personal data for profiling purposes, the school 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 data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

16. Data Protection by design and default and Data Protection Impact Assessments

16.1. The school will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities. In line with the data protection by default approach, the school will ensure that only data that is necessary to achieve its specific purpose will be processed.

16.2. 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.

16.3. 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.

16.4. 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.

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

16.6. The 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

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

17. Data breaches

17.1. All staff **must** report **immediately** to a member of the SLT any suspected data breaches (the loss, theft, unauthorised access to data etc.) and follow up by completing and submitting a data breach form available from the school office. See attached data breach procedure workflow document. It will be for the Bishops' data protection team/DPO to decide whether the suspected data breach warrants reporting to the ICO. NB. a data breach would include the accidental sharing of personal data via a wrongly addressed email.

17.2. 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.

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

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

17.5. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it by the school's Data Protection Officer.

17.6. 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.

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

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

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

17.10. 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

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

17.12 All breaches are recorded on the incidents and breaches log and reported regularly to the governors Resources Committee

18. Data security

18.1. 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.

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

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

18.4. All IT systems - mobile devices, laptops, tablets, mobile phones and any device capable of processing data will be password protected.

A. All IT systems will be kept securely; the server and hard disks will be in a locked cabinet and the server rooms locked at all times other than when accessed by authorised personnel; desktop computers and portable devices will be sited/stored in secure places.
B. Staff are expected to ensure the safety of their allocated school devices. Devices may not be left unattended in cars at any time and they must be kept out of sight if taken home.
C. All passwords must be 'strong;' (at least 8 characters with a mixture of upper- and lower-case letters and numbers), the school will require regular changing of passwords.

18.5. No passwords will be written down or shared; advice is available on the safe storage of passwords.

18.6. The school will devise granulated levels of access as appropriate to staff responsibilities for access to personal data. Devices that are used to process sensitive data and/or are vulnerable to theft will be secured with encryption.

18.7. Where practical computers that might be used to process personal data will be set to lock (a screensaver will activate) after 10 minutes of inactivity.

18.8. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up to an alternate location.

18.9. Technical measures are in place to prevent the use of removable media to take personal data from the school systems. Express permission from the Data & Systems Manager is required in exceptional cases. In these cases encrypted media will be used.

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

18.11. It is understood that staff and governors may use their personal laptops or computers for school purposes, however where this is the case they will ensure that this is done in a secure fashion including but not limited to using password-protection to ensure no unauthorised access of school data..

18.12. Where personal information that could be considered private or confidential is taken off the premises, either in electronic (including uploading to cloud-based storage) 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.

18.13. Emails containing sensitive or confidential information, including personal data are password-protected or encrypted if the email is sent between a member of staff and an external recipient (e.g. another school, agency or parent).

18.14. Schoolcomms is the preferred method of communicating with parents via text or email, however if circular emails to parents are sent by individual members of staff, they are sent using blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

18.15. All deleted personal data will be deleted in a secure manner: physical data will be shredded, and digital data will be fully deleted with trash / junk emptied regularly. Hard disks no longer required will have the data on them deleted and the deletion certified by the ICT equipment recycling contractor. ICT assets will be disposed of in accordance with the ICO's guidance on the disposal of ICT assets.

18.16. 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. Hirers of the school are restricted to agreed areas.

18.17. 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.

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

19. Notification and consent - Biometric data

Please note that the obligation to obtain consent for the processing of biometric information of children under the age of 18 is not imposed by the Data Protection Act 2018 or the UK GDPR. Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

19.1. Where the school uses pupils' biometric data as part of an automated biometric recognition system (e.g. using pupils' fingerprints to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012.

19.2. Prior to any biometric recognition system being put in place or processing a pupil's biometric data, the school will send the pupil's parents a Parental Notification and Consent Form for the use of Biometric Data.

19.3. Written consent will be sought from at least one parent of the pupil before the school collects or uses a pupil's biometric data.

19.4. The name and contact details of the pupil's parents will be taken from the school's admission register.

19.5. Where the name of only one parent is included on the admissions register, the headteacher will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent.

19.6. The school does not need to notify a particular parent or seek their consent if it is satisfied that:

- The parent cannot be found, e.g. their whereabouts or identity is not known.
- The parent lacks the mental capacity to object or consent.
- The welfare of the pupil requires that a particular parent is not contacted, e.g. where a pupil has been separated from an abusive parent who must not be informed of the pupil's whereabouts.
- It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.

19.7. Where neither parent of a pupil can be notified for any of the reasons set out in 6.6, consent will be sought from the following individuals or agencies as appropriate:

- If a pupil is being 'looked after' by the LA or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified, and their written consent obtained.
- If the above does not apply, then notification will be sent to all those caring for the pupil and written consent will be obtained from at least one carer before the pupil's biometric data can be processed.

19.8. Notification sent to parents and other appropriate individuals or agencies will include information regarding the following:

- Details about the type of biometric information to be taken
- How the data will be used
- The parent's and the pupil's right to refuse or withdraw their consent
- The school's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed

19.9. The school will not process the biometric data of a pupil under the age of 18 in the following circumstances:

- The pupil (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data
- No parent or carer has consented in writing to the processing
- A parent has objected in writing to such processing, even if another parent has given written consent

19.10. Parents and pupils can object to participation in the school's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the pupil that has already been captured will be deleted.

19.11. If a pupil objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the school will ensure that the pupil's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the pupil's parent(s).

19.12. Pupils will be informed that they can object or refuse to allow their biometric data to be collected and used via a letter.

19.13. Where staff members or other adults use the school's biometric system(s), consent will be obtained from them before they use the system.

19.14. Staff and other adults can object to taking part in the school's biometric system(s) and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

19.15. Alternative arrangements will be provided to any individual that does not consent to take part in the school's biometric system(s), in line with section 20 of this policy.

20. Alternative arrangements

20.1. Parents, pupils, staff members and other relevant adults have the right to not take part in the school's biometric system(s).

20.2. Where an individual objects to taking part in the school's biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g. where a biometric system uses pupil's fingerprints to pay for school meals, the pupil will be able to use cash for the transaction instead.

20.3. Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service or result in any additional burden being placed on the individual (and the pupil's parents, where relevant).

21. Safeguarding

21.1 The school understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

21.2 The school will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect pupils. The governing board will ensure that staff are:

- Confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'.
- Aware that information can be shared without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a pupil in a timely manner.

21.3 The school will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

21.4 The school will aim to gain consent to share information where appropriate; however, staff will not endeavour to gain consent if to do so would place a child at risk. The school will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

21.5 Pupils' personal data will not be provided where the serious harm test is met. Where there is doubt, the school will seek independent legal advice.

22. Publication of information

21.1. The school will not publish any personal information, including photos, on its website, in social media or in any promotional or marketing publication without the permission of the affected individual or those with parental responsibility.

21.2. When uploading information to the school website, staff are considerate of any metadata or deletions (i.e. hiding of cropped parts of images) which could be accessed in documents and images on the site.

23. CCTV

22.1. The school operates CCTV on the premises and is mindful of the GDPR implications of this. The CCTV code of practice is included as appendix 1.

22.1 Requests for access to CCTV are covered in the CCTV code of practice, for general requests, and the Data Protection Policy, for Subject Access Requests.

24 Cloud computing

24.1 For the purposes of this policy, 'cloud computing' refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the school accessing a shared pool of ICT services remotely via a private network or the internet.

24.2 All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

24.3 If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the school.

24.4 All files and personal data will be encrypted before they leave a school device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DPO immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

24.5 As with files on school devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the school should unauthorised access, deletion or modification occur, and ensure ongoing compliance with the school's policies for the use of cloud computing.

24.6 The school's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

24.7 The DPO will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the school's Data Protection Policy.

- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the school decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the school is prepared to accept that risk.
- Monitor the use of the school's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the headteacher

25. Data retention

25.1. Data will not be kept for longer than is necessary in line with the school's Records & Management Plan

25.2. Data no longer required will be deleted as soon as practicable.

25.3. 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.

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

26. DBS data

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

26.2. Data provided by the DBS will never be duplicated.

26.3. 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.

27. Photographs and moving images

27.1 Consent is requested from parents and staff for the use of images. Communication requesting consent outline the choices that pupils and staff may make for the use of their images.

27.2. The school may seek consent to use photographs for the following purposes:

i. To support school user welfare (identity and security)
ii. To celebrate achievement within the classroom
iii. To celebrate achievement within the school
iv. To celebrate achievement in the printed press
v. To celebrate achievement online

28. Monitoring

The DPO will lead the formal monitoring of the school's compliance with the GDPR. Every member of staff and governor shares a responsibility to monitor compliance and to report any suspected failures to comply.
A monitoring report, to include the record of breaches, subject access requests and freedom of information requests will be brought to Resources Committee once per term.

THE BISHOPS' BLUE COAT CHURCH OF ENGLAND HIGH SCHOOL

CCTV CODE OF PRACTICE

Procedure Name	CCTV Code of Practice
SLT member responsible for Code of Practice	Alison Beasley, Business Manager
Author	Alex Preston, Facilities, Health & Safety Manager and Jonathan Price, Data and Systems Manager
Approved	
Review frequency	2 years

CONTENTS

		Page Number:
1)	Background	25
2)	Location of cameras	26
3)	Notification	26
4)	Storage and retention	26
5)	Access	27
6)	Complaints	28
7)	Staff training	28
8)	Roles and responsibilities	29

APPENDIX A: List of camera locations. **25**

APPENDIX B: Map of camera locations. **26**

1. BACKGROUND

1.1 This code of practice has been written in conjunction with the Data Protection Policy and the Security Policy.

1.2 The Bishops' Blue Coat CofE High School uses closed circuit television (CCTV) images for the prevention, identification and reduction of crime and to monitor the school buildings in order to provide a safe and secure environment for students, staff, contractors and visitors, and to prevent the loss or damage to school property.

1.3 CCTV surveillance at the school is used for the purposes of:

- protecting the school buildings and school assets, both during and after school hours;
- promoting the health and safety of staff, students and visitors;
- preventing bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- ensuring that the school rules are respected so that the school can be properly managed.

1.4 The CCTV system is owned, maintained and operated by the school. Deployment of each is determined by the responsible staff member in section 8.

1.5 The CCTV system comprises of –

i. a number of fixed and pan, tilt, zoom (PTZ) cameras around the site
ii. several Networked Video Recording (NVR) devices located securely in one of our server rooms – this is where the raw footage recorded by all cameras is stored. Footage is automatically deleted within 30 days.
iii. Display monitors located in the Administration Office and the Caretakers Office
iv. Software installed on the PCs of ICT support staff and the Facilities, Health and Safety Manager. This software allows for the monitoring of live footage as well as the 'archiving' of selected sections of live footage for subsequent review.

1.6 The CCTV can be monitored centrally from the school main office, the caretaker's office, the Facilities, Health and Safety Manager's office and the ICT support office by nominated staff.

1.7 The school complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use.

1.8 The use of the CCTV system will be conducted in a professional, ethical and legal manner and any use of CCTV security technologies for purposes other than those listed in section 1.3 above is expressly prohibited by this practice.

1.9CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the school.

2.0 Location of cameras

2.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed, and care will be taken to ensure that reasonable privacy expectations are not violated.

2.2 The school will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act. The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas.

3.0 Notification

3.1 A copy of this CCTV Code of Practice will be provided on request to staff, students, parents and visitors.

3.2 Adequate signage will be on display in reception for use of CCTV on site. Adequate signage will also be prominently displayed at the entrance to The Bishops' Blue Coat CofE High School property.

4.0 Storage, Retention and Archiving

4.1 The images are *stored* on a number of NVRs (see 1.5) located in a server room, with physical access restricted to authorised ICT personnel. The images captured by the CCTV system will be *retained* for a maximum of 30 days, except where the image identifies an issue and is *archived* specifically in the context of an investigation/prosecution of that issue.

4.2 Images and recordings maybe *archived* for subsequent investigation, these archives will be stored in a secured electronic folder with a log of access kept.

4.3 Access to these archived recordings will be restricted to authorised personnel. The nominated staff positions are:

I. Headteacher
II. Deputy Headteacher
III. Business Manager
IV. Facilities, Health and Safety Manager
V. Data & Systems Manager
VI. Assistant ICT Manager
VII. Pastoral Support Officers
VIII. Safeguarding Officers
IX. Year Leaders
X. Senior Year Leader

4.4 In certain circumstances, the archived recordings may also be viewed by other individuals in order to achieve the objectives set out in section 1.3 above. When archived CCTV recordings are being viewed, access will be limited to individuals on a need-to-know basis.

4.5 Footage maybe provided on physical electronic media.

4.6 Archived footage will be deleted from the archive storage area within 30 days unless it is expressly required for ongoing investigation of an incident.

5.0 Access to archived footage

5.1 If staff need to review footage for the purpose of investigation. A log of such access must be recorded stating date and time and subject of the footage plus the date and time it was reviewed and by whom. A log file is kept for this purpose in the secured archive footage area (i.e. T:\CCTV).

5.2 The filesystem will keep an automated log of user accounts used to access any file of CCTV footage.

5.3 In relevant circumstances, CCTV footage may be accessed:

- By the police where The Bishops' Blue Coat CE High School (or its agents) are required by law to make a report regarding the commission of a suspected crime; or
- Following a request by the police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on The Bishops' Blue Coat CE High School, or
- By the HSE and/or any other statutory body charged with child safeguarding; or
- To assist in establishing facts in cases of unacceptable student behaviour; or
- By data subjects (or their legal representatives), pursuant to a Subject Access Request or
- By individuals (or their legal representatives) subject to a court order.
- By the school insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property.

5.4 In the case of access by anyone other than the subject themselves, or school staff, individuals other than the subject, must be redacted.

6.0 Complaints

6.1 Complaints and enquiries about the operation of CCTV will be handled in accordance with the schools complaints policy.

7.0 Staff Training

7.1 Staff authorised to monitor live footage, operate the CCTV system or review archived footage will be trained to comply with this code of practice. Staff will understand that all information relating to the CCTV images must be handled securely.

7.2 Staff will receive appropriate training to enable them to identify and handle different requests according to regulations.

7.3 Staff misuse of surveillance system information may lead to disciplinary proceedings.

8.0 Roles and responsibilities

The Headteacher has overall responsibility, with roles carried out as follows:

8.1 The Business Manager will:

8.1.1 Ensure that the use of CCTV systems is implemented in accordance with the policy set down by The Bishops' Blue Coat CE High School.

8.1.2 Ensure freedom of information requests and subject access requests are dealt with in accordance with legislation and refer to the DPO where necessary.

8.1.3 Refer to the school's DPO with regard to deciding where CCTV is needed to justify its means and with regards to the lawful processing of CCTV footage.

8.1.4 Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within The Bishops' Blue Coat CE High School.

8.1.5 Ensure that the CCTV monitoring at The Bishops' Blue Coat CE High School is consistent with highest standards and protections.

8.1.6 Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.

8.2 The Facilities Health and Safety Manager will:

8.2.1 Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy.

8.2.2 Review camera locations and re-locate/remove/add cameras as required to meet the objectives of this code of conduct.

8.2.3 Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally.

8.2.4 Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place

8.2.5 Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"

8.2.6 Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.

8.3 The Data and ICT manager will:

8.3.1 Maintain a record of access (e.g. an access log) to archived footage, or the release of footage or any material recorded or stored in the system.

8.3.3 Ensure that archived footage is stored in a secure location with access by authorised personnel only.

8.3.4 Ensure that archived footage is stored for a period not longer than 30 days and are then erased unless required as part of an investigation or court proceedings (criminal or civil).

8.3.5 Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics.

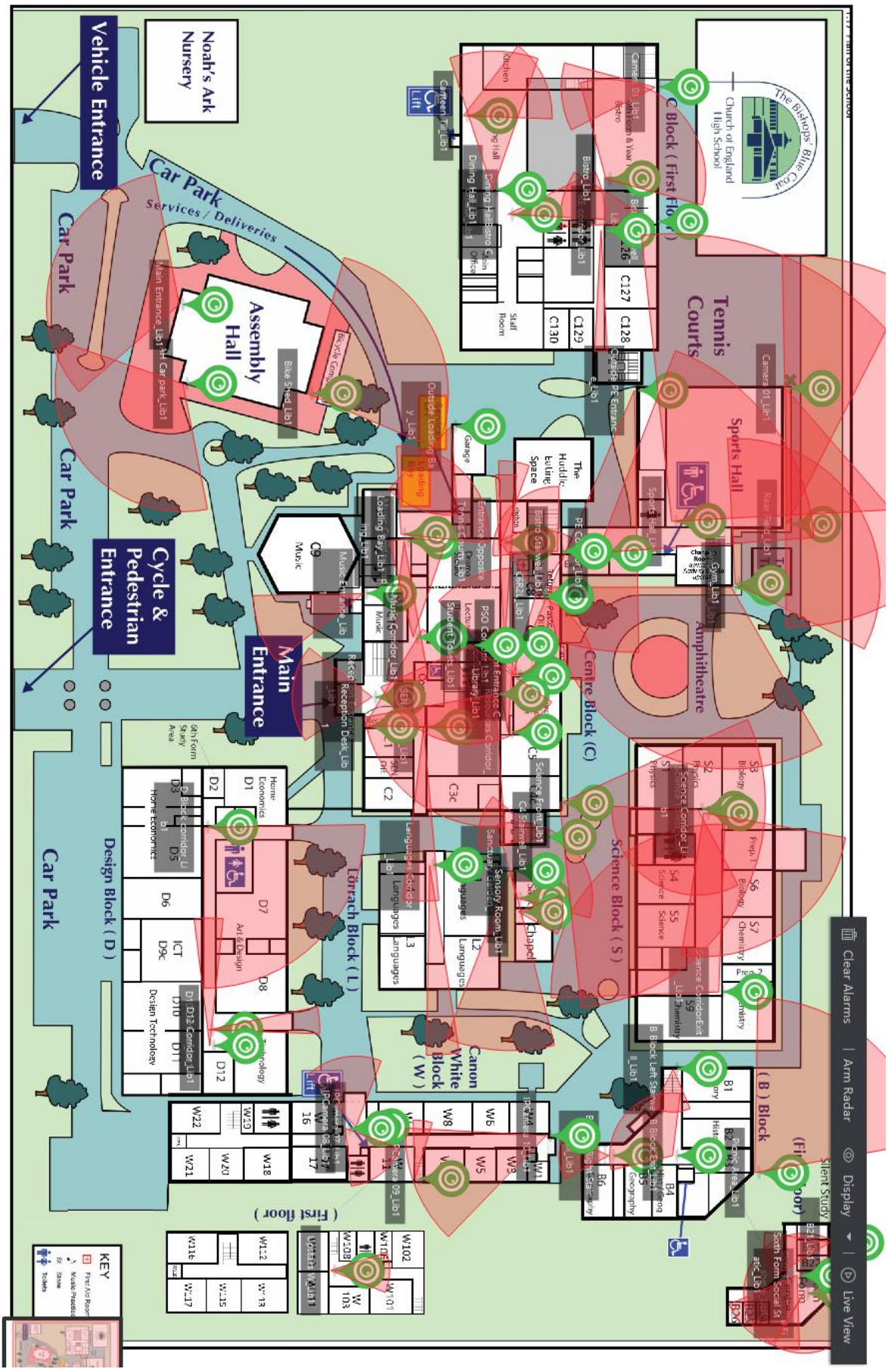
APPENDIX 1A – List of camera locations

Camera No	Description	Int/Ext	Block	NVR
1	Reception Entrance	INT	C	1
2	Reception Desk	INT	C	1
3	Entrance C9	INT	C	1
4	Music Corridor Door	INT	C	1
5	Music Corridor- Loading	INT	C	1
6	Loading Bay	INT	C	1
7	Student Toilet downstairs C	INT	C	1
8	Resources Corridor	INT	C	1
9	Student Entrance rear C	INT	C	1
10	Lower C corridor intersection	INT	C	1
11	PSO Corridor	INT	C	1
12	PE Corridor	INT	C	1
13	Bistro Stairwell	INT	C	1
14	Entrance opposite tennis courts	INT	C	1
15	Sports Hall	INT	C	1
16	Library	INT	C	1
17	SEN Corridor	INT	C	1
18	Languages Corridor	INT	L	1
19	Science Corridor S8-S5	INT	S	1
20	Science Corridor S3	INT	S	1
21	Picnic area	EXT	B	1
22	B4 - Exit	INT	B	1
23	Upstairs W	INT	W	1
24	D10 Entrance	INT	D	1
25	D12 Corridor	INT	D	1
26	C4 Stairwell	INT	C	1
27	Dining Hall/Bistro Corridor	INT	C	1
28	Dining Hall	INT	C	1
29	Bistro	INT	C	1
30	Top Bistro Stairwell	INT	C	1
31	AH Car Park	EXT	AH	1
32	Bike Shed	EXT	AH	1
33	Outside Loading Bay	EXT	C	1
34	Outside PE Entrance	EXT	C	1
35	Amphitheatre from Sports	EXT	C	1
36	Sixth Form Social fisheye	INT	B	1
37	B21	INT	B	1
38	Sixth Form Social static	INT	B	1
39	B Block right stairwell	INT	B	1
40	B Block Left stairwell	INT	B	1
41	R2L	INT	C	1

42	W block entrance	INT	W	1
43	W block corridor outside VBU office	INT	W	1
44	W block corridor from W11	INT	W	1
45	Old W toilets 2	INT	W	1
46	Sanctuary Garden	EXT	T	1
47	Science Front from C	EXT	C	1
48	Science Toilets	INT	S	1
49	Main School Entrance	EXT	A	1
50	Sanctuary	INT	T	1
51	Sensory Room	INT	T	1
52	Outside Gym	EXT	C	1
53	Outside D block toilets	INT	D	1
54	Re corridor	INT	C	1
55	Rear field facing SW	EXT	C	1
56	Rear field facing NW	EXT	C	1
57	Bistro counter	INT	C	1
58	Canteen till	INT	C	1
59	Outside Science Front	EXT	S	2
60	B block approach	EXT	S	2
61	Outside Science to B	EXT	S	2
62	Outside W Main Walkway	EXT	W	2
63	C-L walkway	EXT	C	2
64	New W front	EXT	D	2
65	Staff Car Park	EXT	D	2
66	Staff Car Park	EXT	D	2
67	Student Gate	EXT	D	2
68	Drop Off	EXT	D	2
69	Outside Main Entrance	EXT	D	2
70	Outside Main Entrance To Main	EXT	D	2
71	Music To Parents Car Park	EXT	C	2
72	Tennis Court PTZ	EXT	C	2
73	D/W Car Park PTZ	EXT	D	2
74	Amphitheatre from C	EXT	C	2
75	Top carpark 1	EXT	W	3
76	Top carpark 2	EXT	W	3
77	New W upstairs corridor	INT	W	3
78	New W stairwell	INT	W	3
79	New W downstairs corridor	INT	W	3
80	New Foor counter	INT	C	3
81	New Food Court	INT	C	3
82	New W entrance	INT	W	3
83	New W toilets	INT	W	3
84	D10 rear workshop	INT	D	3
85	D12 workshop	INT	D	3

86	D12 storeroom	INT	D	3
87	Huddle picnic area	EXT	C	3
88	Upper C toilets	INT	C	3
89	Old W toilets	INT	W	3

APPENDIX 1B – Map of camera Locations



APPENDIX 2

Data Breach Procedure

1. Introduction

A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, whether by accidental or deliberate causes".

The General Data Protection Regulation (GDPR) introduces a duty on all organisations to report certain types of personal data breach to the relevant authority.

2. What is a Data Breach

Personal data breaches can include the following:

- access to personal data by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- hand-held devices / laptops containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

3. Practical examples of breaches I should report to the Data Protection Officer (DPO)

- I have lost a USB stick which I was using for my research project, which holds personal information
- My work laptop has been stolen (from work or elsewhere)
- I sent a data file to 'Miss Jones', but it was the wrong 'Miss Jones'
- I sent a letter including someone's bank details to an incorrect address
- I updated a student's address and mobile number, but it was on the wrong profile
- I printed a document which contained personal data, left it on my desk and I cannot locate it.

Examples of personal and sensitive personal data:

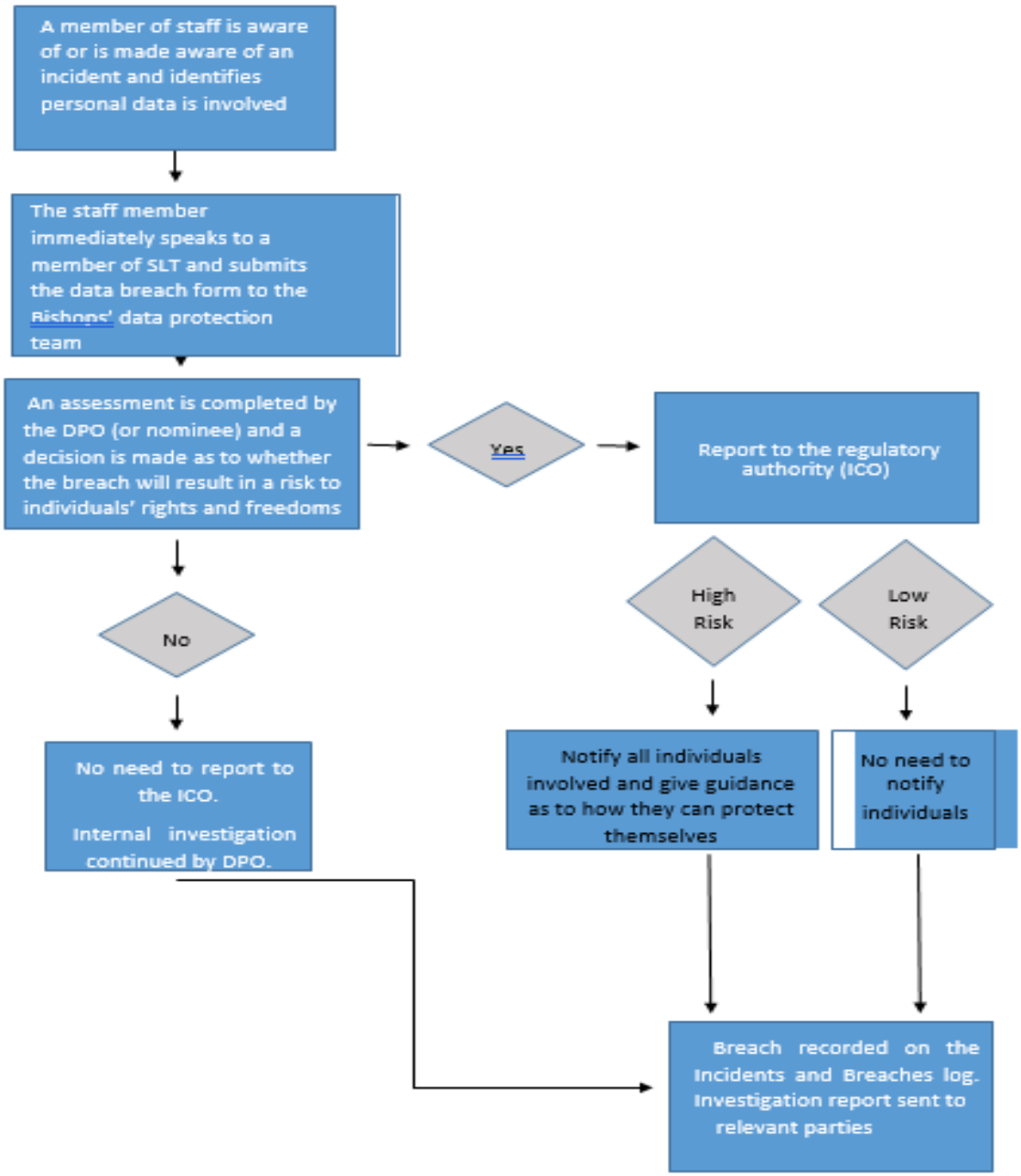
Personal Data	**Sensitive Data**
Full Name	Racial or ethnic origin of the data subject
Date of Birth	Political Opinions
Address	Religious beliefs or beliefs of a similar nature
Postcode	Whether the data subject is a trade union member
Telephone Numbers	Physical, mental health or condition
Email Address	Commission or alleged commission of any offence
Employee/Student ID Number	Any proceedings for any committed or alleged offence, including the disposal or sentence of any court in such proceedings
Driving Licence Number	
Passport Number/NI Number	
Bank Details	

4. Responsibility

It is the responsibility of everyone at The Bishops' Blue Coat Church of England High School to ensure they keep personal data safe. In the event that you are aware of a security breach, you must act fast and ensure you follow the procedure below.

If you believe you may have encountered a data breach, you must **immediately** report to a member of SLT and submit the data breach reporting form below to the data protection team at Bishops' as noted on the form.

Data Breach workflow



DATA BREACH - REPORTING FORM

In the box below, please describe in as much detail as you can, the nature of the personal data breach:

Please fill in the following details:

Your Name:	
Your Department:	
Date of Breach:	
Date of Reporting:	
Approximate number of individuals data concerned:	
Is there any sensitive personal data involved: If YES - please give full details	
Are there any subjects under the age of 18 If YES - approx. how many?	
Have you taken any action to rectify the issue at the time of reporting? If so what action?	

Please send your completed form to the data protection team: abeasley@bishpschester.co.uk ,jprice@bishopschester.co.uk and ssowden@bishopschester.co.uk