BISHOP HEBER HIGH SCHOOL

RESPECT · OPPORTUNITY · ACHIEVEMENT

DATA PROTECTION POLICY (inc. ESAFETY)

Data Protection (CWaC) & ESafety Policy

(Inc. ICT Acceptable Use)

BISHOP HEBER HIGH SCHOOL

RESPECT · OPPORTUNITY · ACHIEVEMENT

DATA PROTECTION POLICY (inc. ESAFETY)

Cheshire West and Chester

School Data Protection Policy

(CWAC Adopted)

BISHOP HEBER HIGH SCHOOL

RESPECT · OPPORTUNITY · ACHIEVEMENT

DATA PROTECTION POLICY (inc. ESAFETY)

Document Control Information	
Document ID	Bishop Heber Data Protection Policy
Document title	Data Protection Policy
Version	1
Status	Draft
Author	Maura Nesbitt, Business Manager (CWaC Adopted)
Publication date	January 2019
Next review date	June 2020

Version History			
Version	**Date**	**Detail**	**Author**
1.0			

Approvals	
Approver	**Date**

DATA PROTECTION POLICY (inc. ESAFETY)

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

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

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

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

The school needs to identify what additional policies they have that operate alongside this policy. This could include:

- *Records Management and Retention Policy*
- *IT Acceptable Use Policy*
- *CCTV Policy*
- *Information Rights Policy*

2. Applicable data

For the purpose of this policy:

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, 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 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.

2.4 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.

2.5 Data Controller is usually an organisation who dictates the reason and purpose for how data is processed. The Council itself is a Data Controller as it chooses how it collects, uses and shares its own data.

2.6 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 Data Protection Act, this can be anything up to £500,000. Under the General Data Protection Regulation this can be up to €20 Million or 4% of a company's global turnover.

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

Technical Measures

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

Organisational Measures

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

4.2. Bishop Heber High School will provide comprehensive, clear and transparent privacy notices.

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, we shall maintain a record of processing activities will include as a minimum the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures

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

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

5. Data protection officer (DPO)

5.1. Bishop Heber High School has appointed a DPO in order to:

- Inform and advise Bishop Heber High School and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor Bishop Heber High 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. Bishop Heber High School will make freely available the contact details for their appointed DPO:

Schools Data Protection Officer
Cheshire West and Chester Council,
HQ, 58 Nicholas Street,
Chester,
CH1 2NP

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 your 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 you process.

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

- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

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

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

7. Consent

7.1. Where there is no other legal basis for the processing of data Bishop Heber High 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 previously accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

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

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

8. The right to be informed

8.1. 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.

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. A form for requesting information is available from the school.

9.3. Bishop Heber High School will verify the identity of the person making the request before any information is supplied as well as confirming the subject of the request and the right to make such a request (see 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.

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

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

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

9.14. The school will clearly communicate and promote the process for the submission of Subject Access Requests and the exercising of other individual rights as defined under the GDPR during holiday periods, stating clearly how the school will handle these requests and how this may impact on any time scales.

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.

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

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority

- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

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.

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. Bishop Heber High School will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

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

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. Privacy by design and Data Protection Impact Assessments

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

15.2. 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.

15.3. 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.

15.4. 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.

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

15.6. Bishop Heber High School will ensure that all DPIAs include the following information:

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

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

16. Data Processors

16.1 Bishop Heber High School will ensure that whenever it employs or utilises a data processor a written contract will be in place.

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

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

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

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

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

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

17. Data breaches

17.1. 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.

17.2. Bishop Heber High 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.

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

17.4. 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.

17.5. 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.

17.6. 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.

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

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

17.9. Effective and robust breach detection, investigation and internal reporting procedures 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.

18. Data security

[NOTE: SCHOOLS WILL HAVE TO DETERMINE WHAT LEVELS OF SECURITY THEY ARE COMFORTABLE WITH AND AMMEND THIS SECTION (ALL OF 18) ACCORDINGLY]

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

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

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

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

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

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

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

18.8. Staff and Governors will not use their personal laptops or computers for school purposes.

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

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

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

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

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

18.14. 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.

18.15. 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.

18.16. 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.

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

19. Publication of information

19.1. Bishop Heber High 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.

19.2. When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

20. CCTV

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

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

21. Data retention

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

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

21.3. 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.

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

22. DBS data

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

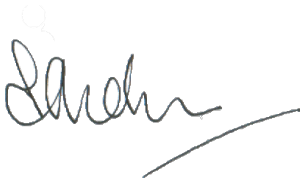
22.2. Data provided by the DBS will never be duplicated.

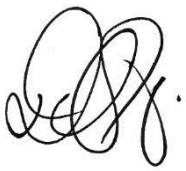
22.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

23. Policy review

23.1. This policy is reviewed annually.

23.2. The next scheduled review date for this policy is May 2019





Signed: (Chair of Governors) **(Headteacher)**

Administration Use:

BISHOP HEBER HIGH SCHOOL

RESPECT · OPPORTUNITY · ACHIEVEMENT

DATA PROTECTION POLICY (inc. ESAFETY)

Statutory/Non-Statutory:	Statutory
Website:	Yes
GB Committee:	REP
Approval Level – Sub Committee or FGB:	Sub Committee (REP)
Review:	Annually
Document Formulated:	January 2016
Date Reviewed Document Approved by REP:	21st March 2022
Date FGB to be Advised of Reviewed Document:	13th June 2022
Next Review Date:	January 2023
	Under Review January 2022 (delayed due to Covid)

BISHOP HEBER HIGH SCHOOL ESAFETY POLICY

ESAFETY & DATA PROTECTION POLICY

Contents

GUIDANCE 24
INTRODUCTION....25
MONITORING....26
BREACHES 27
Incident Reporting....27
ACCEPTABLE USE AGREEMENT: STUDENTS 28
ACCEPTABLE USE AGREEMENT 29
ACCEPTABLE USE AGREEMENT: STAFF AND VISITORS 30
ACCEPTABLE USE AGREEMENT: GOVERNORS 31
LAPTOP AGREEMENT FOR STAFF 32
COMPUTER VIRUSES 33
Ransomware....33
DISPOSAL OF REDUNDANT ICT EQUIPMENT POLICY....34
E-MAIL 35
Managing e-Mail 35
Receiving e-Mails....36
Sending e-Mails 36
e-mailing Personal, Sensitive, Confidential or Classified Information 36
EQUAL OPPORTUNITIES: STUDENTS WITH ADDITIONAL NEEDS 37
ESAFETY....38
eSafety - Roles and Responsibilities....38
eSafety in the Curriculum....38
eSafety Skills Development for Staff 39
Managing the School eSafety Messages 39
INCIDENT REPORTING, ESAFETY INCIDENT LOG & INFRINGEMENTS....40
Incident Reporting....40
Misuse and Infringements....40
INTERNET ACCESS....41
Managing the Internet 41
Internet Use 41
Infrastructure....42

ESAFETY & DATA PROTECTION POLICY

MANAGING OTHER WEB 2.0 (SOCIAL MEDIA) TECHNOLOGIES 43
PARENTAL INVOLVEMENT 44
PASSWORDS AND PASSWORD SECURITY 45
Passwords 45
Password Security 45
REMOTE ACCESS 47
SAFE USE OF IMAGES 48
Taking of Images and Film 48
Publishing Student's Images and Work 48
Storage of Images 49
Webcams and CCTV 49
Video Conferencing 49
SCHOOL ICT EQUIPMENT 50
Mobile Technologies 50
Personal Mobile Devices (including phones) 51
SERVERS 52
APPENDICES 53
LEGISLATIVE POWERS AT THE TIME OF APPROVAL 54
RELEVANT GOVERNMENT GUIDANCE AT THE TIME OF APPROVAL 55

ESAFETY & DATA PROTECTION POLICY

Guidance

Once this Policy has been ratified by the School's Governors it will be issued to all personnel, including Governors involved in the working of the School.

The Acceptable Use of ICT Agreement will be issued to the appropriate user for signature and collated by a designated member of staff.

The School will ensure that all persons, including Governors, who join the establishment mid-year are provided with this Policy and agreement.

ESAFETY & DATA PROTECTION POLICY

Introduction

Information and Communications Technology in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments [VLE's]
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Laptops, Mobile/ Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently monitored. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At ***Bishop Heber High School*** we understand the responsibility to educate our students on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this Policy and the Acceptable Use Agreement are inclusive of both fixed and mobile internet; technologies provided by the School (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto School premises (such as laptops, mobile phones, tablets and portable media players, etc).

Monitoring

Authorised ICT staff [as determined by the Headteacher] may inspect any ICT equipment owned or leased by the School at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please contact the Network Manager. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the General Data Protection Regulations, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998/General Data Protection Regulations, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of Policy by a School employee, contractor or student may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any Policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

The ICO's [Information Commissioner's Office] has powers to issue monetary penalties up to €20 million for serious breaches.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under GDPR;
- Conduct audits to assess whether organisations processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

Incident Reporting

Any breach must be reported to the Data Protection Lead (DPL) Business Manager or the Strategic Network Manager, we then have 72 hours to decide if we must notify the ICO of the breach.

ESAFETY & DATA PROTECTION POLICY

Acceptable Use Agreement: Students

- I will only use ICT systems in School, including the internet, e-mail, digital video, mobile technologies, etc. for School purposes.
- I will not download or install software on School technologies.
- I will only log on to the School network/ Learning Platform with my own user name and password.
- I will follow the Schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will make sure that all ICT communications with Students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal (this can include photographs, images, videos, emails, and sound clips). If I accidentally come across any such material I will report it immediately to my Teacher, Tutor or Head of Year
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a School project approved by my teacher.
- Images of Students and/or staff will only be taken with the permission of the person involved and will be stored and used for School purposes in line with School Policy**.** Images should not be distributed outside the School network without the permission of the Headteacher.
- I will ensure that my online activity, both in School and outside School, will not cause my School, the staff, Students or others distress or bring into disrepute.
- I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the School community
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to appropriate staff.
- I understand that these rules are designed to keep me safe and that if they are not followed, School sanctions will be applied and my parent/ carer may be contacted.

Please refer to the Behaviour & Discipline Policy for more information

Acceptable Use Agreement

Dear Parent/ Carer

Information Communications Technology including the internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our School. We expect all Students to be safe and responsible when using any ICT. It is essential that Students are aware of eSafety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their Form Tutor or with the Business Manager.

Please return the reply section of this form to School to complete registration.

✂ - - -

ESAFETY & DATA PROTECTION POLICY

Acceptable Use Agreement: Staff and Visitors

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in School. This Policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this Policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the School eSafety coordinator or Data Protection Lead.

- Only equipment explicitly approved by the Network Strategy Manager may be used on the School network
- I will only use the School's ICT systems for work related purposes during the School day
- I will **only** use the School's email / Internet / Intranet / Learning Platform for work related communications
- I will not use social networking sites [e.g. Facebook] to communicate with students without the explicit permission of the Headteacher.
- I will comply with the ICT system security and not disclose any passwords provided to me by the School or other related authorities
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to students.
- I will only use the approved, secure e-mail system(s) for any School business.
- I will ensure that personal data (such as data held on SIMS software) is kept secure and is used appropriately, whether in School, taken off the School premises or accessed remotely.
- I will not install any hardware of software without permission of Network Strategy Manager
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory or which is inappropriate to a School environment.
- Images of students and/ or staff will only be taken, stored and used for professional purposes in line with School Policy. Images will not be distributed outside the School network without the permission of the parent/ carer or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the School community
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in School and outside School, will not bring my professional role or school into disrepute.
- I will support and promote the School's e-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the School

Signature …….…… Date ……

Full Name …….....(printed)

ESAFETY & DATA PROTECTION POLICY

Acceptable Use Agreement: Governors

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in School. This policy is designed to ensure that all Governors are aware of their professional responsibilities when using any form of ICT. All Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Clerk to Governors, who will seek further advice as appropriate.

- Only equipment explicitly approved by the Network Strategy Manager may be used on the School network.
- I will not use the School's e-mail, internet, intranet or learning platform and any related technologies for anything other than Governing matters.
- I will only use the School's e-mail, internet, intranet or learning platform for matters pertaining to Governance, which involve any personal details relating to staff or students.
- I will not use social networking sites (e.g. Facebook) to communicate with students without the explicit permission of the Headteacher.
- I will comply with the ICT system security and not disclose any passwords provided to me by the School or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to students or their families unless personally known.
- I will only use the approved, secure e-mail system(s) for any School business.
- I will ensure that personal data is kept secure and is used appropriately, whether in School, taken off the School premises or accessed remotely.
- I will not install any hardware or software on School equipment, without permission of the Network Strategy Manager.
- Governors should not take any images of any student within School, whether known to them personally or not.
- I understand that all my use of the School internet and other related technologies can be monitored and logged and can be made available, on request through the Clerk to Governors, to the Headteacher (all requests are logged and subject to GDPR/Data Protection Act).
- I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the School community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in School and outside School, will not bring my professional role or School into disrepute.
- I will support and promote the School's e-Safety and Data Security policies.
- I understand this forms part of the Governing Code of Conduct.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the School.

Signature …….……. Date ……
Full Name ……..……..…… (printed)

Laptop Agreement for Staff

The laptop is issued to you for the following purposes:

- To access your email on a daily basis
- To complete online registration and reports
- To support teaching and learning, including the use of the VLE

You will be responsible for the security of the confidential information which can be accessed by or stored on your machine. All sources of such data should be protected by a secure password (minimum of 8 characters including at least one letter and one number) and must be protected from the sight of students or the possibility of unauthorised access (see Data Protection Policy for more information).

The school's insurance policy covers the laptop against theft whilst it is in school, provided that it is not left unattended. It is also covered when taken out of school, provided that the equipment is locked away, out of sight and not left unattended.

Please read the following agreement carefully before signing:

I understand that the laptop is being loaned to me for use in school and at home according to the acceptable use policy laid out by the school (attached). I understand the laptop remains the property of Bishop Heber High School at all times and that it is to be returned on completion of my contract with the school.

I understand that I must return the laptop when requested for maintenance work and that I must not install any programs without the approval of the network manager (approval must be requested by email to naylorg@bishopheber.cheshire.sch.uk). I undertake not to store any materials on the machine which would infringe the copyright of such materials. Extended absence of more than four weeks may require the member of staff to return their laptop to support teaching and learning.

I will be responsible for the care and safety of the machine and will take all reasonable precautions to ensure that it does not become damaged or lost. I understand that I will be liable for the cost of replacing or repairing a machine which has been lost, stolen or damaged as a result of negligence on my part.

I shall be solely liable for and shall indemnify the Council, Bishop Heber High School and Governors against any expense, liability, loss, claim or proceedings whatsoever or howsoever arising under any statute or at common law in respect of personal injury to or the death of any person arising out of or in the course of my use of the laptop.

I shall be liable for and shall indemnify the Council, Bishop Heber High School and Governors against any expense, liability, loss, claim or proceedings in respect of any injury or damage whatsoever to any property real or personal in so far as such injury or damage arises out of or in the course of my use of the laptop and to the extent that the same is due to my negligence, omission or default.

Signature …….…….. Date …… Full Name …… (printed)

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. Data Stick, CD) must be checked for any viruses using School provided anti-virus software before using them

- Never interfere with any anti-virus software installed on School ICT equipment that you use

- The School Antivirus solution is cloud based so updates will occur whenever you have an Internet connection

- If you suspect there may be a virus on any School ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Ransomware

The school has protection in place for ransomware attacks which will protect your laptop whether in school or at home. If you have any concerns, please contact the Network Strategy Manger.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen

- Disposal of any ICT equipment will conform to:

  The Waste Electrical and Electronic Equipment Regulations 2006

  The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

  http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

  http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

  http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

  Data Protection Act 1998 (and General Data Protection Regulation 2018)

  http://www.ico.gov.uk/what_we_cover/data_protection.aspx

  Electricity at Work Regulations 1989

  http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The School will maintain a comprehensive inventory of all its ICT equipment including a record of disposal

- The School's disposal record will include:

  - Date item disposed of
  - Authorisation for disposal, including: verification of software licensing, Approval of the write-off of the equipment by the Finance and Personnel sub-committee
  - How it was disposed of e.g. waste, gift, sale
  - Name of person & / or organisation who received the disposed item

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

e-Mail

The use of e-mail within most Schools is an essential means of communication for staff, students and families. In the context of School, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between Schools on different projects, be they staff based or student based, within School or international. We recognise that Students need to understand how to style an e-mail in relation to their age and good etiquette.

Managing e-Mail

- The School gives all staff their own e-mail account to use for all School business as a work based tool.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The School email account should be the account that is used for all School business
- Staff should not contact Students, parents or conduct any School business using their personal e-mail addresses without the permission of the Headteacher.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on School headed paper
- Students may only use School approved accounts on the School system
- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
- The forwarding of chain letters is not permitted in School.
- All student e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform (the eSafety co-ordinator/ line manager) if they receive an offensive e-mail
- Students are introduced to e-mail as part of the ICT Scheme of Work
- However you access your School e-mail all the School e-mail policies apply
- The use of personal email accounts for sending, reading or receiving school related e-mail is not permitted.

Receiving e-Mails

- Check your e-mail regularly
- Never open attachments from an untrusted source; Consult the Network Manager first.

Sending e-Mails

- Use your own School e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- An outgoing e-mail greater than ten megabytes (including any attachments) will be stopped automatically. This size limit also applies to incoming e-mail
- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section e-mailing Personal, Sensitive, Confidential or Classified Information

e-mailing Personal, Sensitive, Confidential or Classified Information

- Where your conclusion is that e-mail must be used to transmit such data:
- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify the details of a requestor before responding to e-mail requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
    - Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)
    - Provide the encryption key or password by a separate contact with the recipient(s) where possible
    - Do not identify such information in the subject line of any e-mail
    - Request confirmation of safe receipt

Equal Opportunities: Students with Additional Needs

The School endeavours to create a consistent message with parents for all Students and this in turn should aid establishment and future development of the Schools' eSafety rules.

However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

ESAFETY & DATA PROTECTION POLICY

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the School, the Headteacher and governors have ultimate responsibility to ensure that the Policy and practices are embedded and monitored. The named eSafety co-ordinator in this School is the Network Strategy Manager. All members of the School community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance

Senior Management and Governors are updated by the Data Protection Lead and all governors have an understanding of the issues and strategies at our School in relation to local and national guidelines and advice.

This Policy, supported by the School's Acceptable Use Agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole School community.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the students on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The School has a framework for teaching internet skills in ICT lessons.
- The School provides opportunities within a range of curriculum areas to teach about eSafety
- Educating Students on the dangers of technologies that maybe encountered outside School is done informally when opportunities arise and as part of the eSafety curriculum
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Students are taught in Key Stage 3 about copyright and respecting other people's information, images, etc through discussion, modeling and activities
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline
- Students are taught to critically evaluate materials and learn good searching skills through cross

curricular teacher models, discussions and via the ICT curriculum (***Year 8 ICT units)***

- **Case Study work from year 10-13 PHSCE:** covering issues such as sexuality, privacy, reputation and employment

eSafety Skills Development for Staff

- New staff receive information on the School's Acceptable Use Policy as part of their induction [Staff Handbook]
- All staff have been made aware on a regular basis of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the School community (see enclosed flowchart) [**CPD**]
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas [**CPD]**

Managing the School eSafety Messages

- We endeavor to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- eSafety posters will be prominently displayed

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the School's eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other Policy non-compliance must be reported to your Senior Information Risk Owner. See Page 30.

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Where those incidents involve child protection then reports should be made to directly Educational Needs Coordinator (ENCo) or Headteacher as is appropriate. Incidents should be logged.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator. Infringements by staff, depending on the seriousness of the offence; may be investigated by the Headteacher. Very serious offences may lead to immediate suspension, possibly leading to dismissal and involvement of police
- Users are made aware of sanctions relating to the misuse or misconduct through, in the case of student, a note to their Form Tutor. Their account will be blocked and the student required to discuss their misconduct with the Senior Information Risk Officer (SIRO) [Business Manager]. More serious issues will involve the notification of the Year Leader and may involve the ENCO and/or Headteacher depending on the child protection implications of the misuse.
- Staff will be informed of minor infringements of the acceptable use Policy by the Network Strategy Manager. More serious issues will be reported directly to the Headteacher who will then decide the most appropriate way to proceed.

ESAFETY & DATA PROTECTION POLICY

Internet Access

The internet is an open communication medium, available to everyone at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **network** is logged and the logs are regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The School maintains students who will have supervised access to Internet resources (where reasonable) through the School's fixed and mobile internet technology
- Staff must preview any materials before use
- Raw image searches are discouraged when working with students
- All users must observe software copyright at all times. It is illegal to copy or distribute School software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience
- Don't reveal names of colleagues, students or any other confidential information acquired through your job on any social networking site or blog
- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion on what internet activities are permissible for staff and students and how this is disseminated.

ESAFETY & DATA PROTECTION POLICY

Infrastructure

- Our School employs web filtering which is the responsibility of the Network Strategy Manager
- The School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998, General Data Protection Regulations
- Staff and Students are aware that School based email and internet activity can be monitored and explored further if required
- The School does not allow students access to internet logs
- The School uses management control tools for controlling and monitoring workstations
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-Safety Coordinator or teacher as appropriate
- It is the responsibility of the School, by delegation to the Network Manager, to ensure that Anti-virus protection is installed and kept up-to-date on all School machines
- Students and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the School's responsibility nor the Network Manager's to install or maintain virus protection on personal systems.
- Students and staff are not permitted to download programs or files on School based technologies without seeking prior permission from the Network Strategy Manager
- If there are any issues related to viruses or anti-virus software, the Network Manager should be informed immediately by email/ SMS

Managing Other Web 2.0 (Social Media) Technologies

Web 2.0, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our Students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the School endeavours to deny access to social networking sites to students within School
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, School details, IM/ email address, specific hobbies/ interests)
- Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts online
- Our students are asked to report any incidents of bullying to the School as soon as possible after it has occurred.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with Students using VLE or other systems approved by the Headteacher

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of School and also to be aware of their responsibilities. We consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to School
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on School website)
- The School disseminates information to parents relating to eSafety where appropriate in the form of;
    - Posters/booklets
    - Website/ Learning Platform postings
    - Newsletter items

Passwords and Password Security

Passwords

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- User ID and passwords for staff and Students who have left the School are disabled after their last day at Bishop Heber High School

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team.

Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The Students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and Students are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the School's e-safety Policy and Data Security
- Users are provided with an individual network, email, Learning Platform and Management Information System log-in username.
- Students are not allowed to deliberately access on-line materials or files on the School network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of School networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

- In our School, all ICT password policies are the responsibility of the Network Strategy Manager and all staff and students are expected to comply with the policies at all times

Remote Access

- You are responsible for all activity via your remote access facility
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment
- The school staff now have to use multifactor authentication for remote access.
- (Multifactor authentication (MFA) adds a layer of protection to the sign-in process. When accessing accounts or apps, users provide additional identity verification by entering a code received by their phone)

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the School community or public, without first seeking consent and considering the appropriateness.

- Parents opt-in to give consent for unnamed images of their children to be used on the VLE/ Website. Staff must check on a student's status with the Main School Office prior to posting. Express parental permission must be sought for the use of named images.

- Students are not permitted to use personal digital equipment to record images of the others without the express permission of staff and of those being photographed, this includes when on field trips.

Publishing Student's Images and Work

On a child's entry to the School, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the School web site

- on the School's Learning Platform

- in the School Prospectus and other printed publications that the School may produce for promotional purposes

- recorded/ transmitted on a video or webcam

- in display material that may be used in the School's communal areas

- in display material that may be used in external areas, such as exhibition promoting the School

- in general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this School unless specifically withdrawn by the Legal Guardian. Parents/ carers may withdraw permission, in writing, at any time.

Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of Students will not be published without the express written permission of the student's Legal Guardian.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. Only the Network Strategy Manager and SLT have authority to approve upload to the site.

Storage of Images

- Images/ films of children are stored on the School's network
- ***The IAO*** has the responsibility of deleting the images when they are no longer required, or the student has left the School

Webcams and CCTV

Possible statements

- The School uses CCTV for security and safety. The Network Strategy Manager is responsible for authorising access. Notification of CCTV use is displayed at the front of the School. Please refer to the hyperlink below for further guidance http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx
- We do not use publicly accessible webcams in School
- Misuse of the webcam by any member of the School community will result in sanctions (as listed under the 'inappropriate materials' section of this document)

Video Conferencing

- All students are supervised by a member of staff when video conferencing
- All students are supervised by a member of staff when video conferencing with end-points beyond the School
- The School keeps a record of video conferences, including date, time and participants.
- The School conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be CRB checked
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the School's ICT equipment provided to you
- The School logs ICT equipment issued to staff and records serial numbers as part of the School's inventory
- Do not allow your visitors to plug their ICT hardware into the School network points (unless special provision has been made).
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the School's network drive. You are responsible for the backup and restoration of any of your data that is not held on the School's network drive
- Privately owned ICT equipment should not be used on a School network without express permission from the Network Strategy Manager
- On termination of employment, resignation or transfer, return all ICT equipment to the Network Manager.
- Please refer to the data protection policies for more information on keeping data secure and the processes we follow.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for students. Many existing mobile technologies such as portable media players, Personal Digital Assistants (PDAs), gaming devices, mobile and smart phones are familiar to students outside of School too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in School is allowed. Our School chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

ESAFETY & DATA PROTECTION POLICY

Personal Mobile Devices (including phones)

- The School allows staff to bring in personal mobile phones and devices for their own use.
- Students are allowed to bring personal mobile devices/phones to School but must not use them within lesson time, unless directed by a member of staff. Students may use mobile phones during breaks, lunchtimes and study periods in designated locations
- Permission must be sought from a member of teaching staff before any image or sound recordings are made on these devices by students.
- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer
- The School is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages, explicit photographs, videos/audio recordings of defamatory or derogatory nature between any member of the School community (including out of School hours) is not allowed
- Users bringing personal devices into School must ensure there is no inappropriate or illegal content on the device
- Students on exchange visits will follow the OEAP National Guidance in accordance with the School's Trips and Visits Policy.
- Breaches of these guidelines may result in disciplinary action (in line with the School's Behaviour and Discipline Policy).

Please refer to the Behaviour and Discipline Policy for more information

Servers

- Are always kept in a locked and secure environment?
- Have limited access rights
- Servers have security software installed appropriate to the machine's specification
- Backups are encrypted
- Data is backed up regularly
- Remote backups are automatically encrypted

Appendices

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website

http://www.ico.gov.uk/

Data Protection Act – data protection guide, including the 8 principles

http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

GDPR

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

PC Disposal – SITSS Information

http://www.thegrid.org.uk/info/traded/sitss/computers/pc_disposal.shtml

ESAFETY & DATA PROTECTION POLICY

LEGISLATIVE POWERS AT THE TIME OF APPROVAL

Education Act 1996

School Standards and Framework Act 1998

Education Act 2002

Education and Inspections Act 2006

School Information (England) Regulations 2008

Equality Act 2010

Schools (Specification and Disposal of Articles) Regulations 2012

ESAFETY & DATA PROTECTION POLICY

RELEVANT GOVERNMENT GUIDANCE AT THE TIME OF APPROVAL

https://www.gov.uk/government/collections/data-protection-act-2018

https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf