Adopted by Full Governing Body on 31.03.2022 Item 9a

Data Protection Policy

Whitley Bay High School

March 2022

DATA PROTECTION POLICY

1.0 Introduction

Whitley Bay High School Data Protection Policy has been produced to ensure compliance with the General Data Protection Regulation (GDPR) and associated legislation, and incorporates guidance from the Information Commissioner's Office (ICO).

The Data Protection Policy gives individuals rights over their personal data and protects individuals from the erroneous use of their personal data.

Whitley Bay High School is registered with the ICO (ICO registration number: Z8845007) as a Data Controller for the processing of living individuals' personal information.

2.0 Purpose

Whitley Bay High School Data Protection Policy has been produced to ensure its compliance with the GDPR laws brought into place in 2018.

The Policy incorporates guidance from the ICO and outlines the School's overall approach to GDPR including its responsibilities and individuals' rights.

3.0 Scope

This Policy applies to all employees (including temporary, agency staff and contractors, consultants and suppliers working for, or on behalf of, the School), governors, third parties and others who may process personal information on behalf of the School.

The Policy also covers any staff, governors, pupils and parents who may be involved in research or other activity that requires them to process or have access to personal data, for instance as part of a research project or as part of professional practice activities. If this occurs, it is the responsibility of the School to ensure the data is processed in accordance with GDPR and that pupils and staff are advised about their responsibilities.

4.0 Data covered by the Policy

A detailed description of this definition is available from the ICO, however briefly; personal data is information relating to an individual where the structure of the data allows the information to be accessed i.e. as part of a relevant filing system. This

includes data held manually and electronically and data compiled, stored or otherwise processed by the School, or by a third party on its behalf.

Special category data is personal data consisting of information relating to:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

5.0 The Six Data Protection Principles

GDPR requires Whitley Bay High School, its staff and others who process or use any personal information to comply with the six data protection principles.

The principles require that personal data shall be:

1) processed lawfully, fairly and in a transparent manner in relation to individuals;

2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4) accurate and, where necessary, kept up to date;

5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

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

6.0 Responsibilities

Whitley Bay High School has an appointed Data Protection Officer to handle day-to-day issues which arise, and to provide members of the School with guidance on Data Protection issues to ensure they are aware of their obligations.

All new staff will be required to complete mandatory information governance training as part of their induction and existing staff will be required to undertake refresher training on a regular basis as part of Safeguarding Training.

All employees at Whitley Bay High School have access to a secure account and email via Office 365. The majority of roles within the school involving sensitive data and information can be carried out using these professional accounts. Therefore, staff must check with the Data Protection Officer or a member of the Senior Leadership Team if they intend to use other applications or programmes involving school information.

Employees and Governors of Whitley Bay High School are expected to:

- Familiarise themselves and comply with the six data protection principles.
- Ensure any possession of personal data is accurate and up to date.
- Ensure their own personal information is accurate and up to date.
- Keep personal data for no longer than is necessary in line with retention guidelines.
- Ensure that any personal data they possess is secure and in compliance with Whitley Bay High School's information related policies and strategies.
- Acknowledge data subjects' rights (e.g. right of access to ***all*** their personal data held by Whitley Bay High School) under GDPR, and comply with access to those records.
- Ensure personal data is only used for those specified purposes and is not unlawfully used for any other business that does not concern Whitley Bay High School.
- Obtain consent when collecting, sharing or disclosing personal data. Students will be asked whether they have opted out of giving their consent when publishing information online.
- Read section 9 of the E-Safety Policy to ensure they:
    - Take care to ensure the safe keeping of personal data stored on both hardware and software, minimising the risk of its loss or misuse.
    - Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data. The school will automatically lock any screen after 5 minutes.
    - Transfer data using encryption and secure password protected devices.
- When storing personal data on any portable computer system, mobile device, memory stick or any other removable media, staff must ensure:
    - The data must be encrypted and password protected.

    - The device must be password protected. (many memory sticks / cards and other mobile devices cannot be password protected – staff have the responsibility to check anything they may use)
    - The device must offer approved virus and malware checking software.
    - The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.
- Take care when contacting a student, parent, or guardian, to ensure they are using the correct contact details – this includes checking phone numbers via SIMS for calls, and double-checking they have selected the correct recipient for an e-mail, letter or text. When e-mailing a generic message to 2 or more recipients, the 'bcc' option on e-mails must be selected so as not to send parental e-mail addresses to other parents.
- Contact the Data Protection Officer for any concerns or doubt relating to data protection to avoid any infringements of GDPR 2018.

Pupils, of Whitley Bay High School are expected to:

- Comply with the six data protection principles
- Comply with any security procedures implemented by Whitley Bay High School.
- Complete their consent regarding the use of their personal data on induction to the school. All of our pupils are over 13 on admission, therefore can consent without parental feedback.
- Notify the school Data Protection Officer that they do not consent to the sharing of their data (in any form) online on the school website and social media accounts. An example could be when part of a team photo with the intended use of sharing this on the school Twitter account.

7.0 Obtaining, Disclosing and Sharing

Only personal data that is necessary for a specific School related business reason should be obtained.

Pupils and their parents and or Carers will be informed about how their data will be processed.

Upon acceptance of employment at Whitley Bay High School, members of staff also consent to the processing and storage of their data.

Data must be collected and stored in a secure manner as detailed in section 6 and in the school's E-Safety Policy section 9.

Personal information must not be disclosed to any third party organisation without prior consent of the individual concerned. This also includes information that would confirm whether or not an individual is or has been an applicant, pupil or employee of Whitley Bay High School.

Whitley Bay High School may have a duty to disclose personal information in order to comply with legal or statutory obligations. GDPR allows the disclosure of personal data to authorised bodies, such as the police and other organisations that have a crime prevention or law enforcement function.

Personal information that is shared with third parties on a more regular basis shall be carried out under written agreement to stipulate the purpose and boundaries of sharing. For circumstances where personal information would need to be shared in the case of ad hoc arrangements, sharing shall be undertaken in compliance with GDPR 2018.

8.0 Retention, Security and Disposal

Recipients responsible for the processing and management of personal data need to ensure that the data is accurate and up-to-date. If an employee, student or applicant is dissatisfied with the accuracy of their personal data, then they must inform Whitley Bay High School.

Personal information held in paper and electronic format shall not be retained for longer than is necessary. In accordance with Article 5 of the General Data Protection Regulations, personal information shall be collected and retained only for business, regulatory or legal purposes.

In accordance with the provisions of the GDPR, all staff whose work involves processing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage and ensure appropriate measures are in place to prevent accidental loss or destruction of, or damage to, personal data.

In accordance with Whitley Bay High School E-Safety Policy, staff working from home will be responsible for ensuring that personal data is stored securely and is not accessible to others. We advise no data is stored on any home device, but expect staff to follow the guidelines outlined above in Section 6 and within the E-Safety Policy section 9.

All departments should ensure that data is destroyed in accordance with the Information and Records Management Society (IRMS) toolkit Retention Schedule when it is no longer required. This follows guidance from the DfE and the Schedule, taken from the IRMS Toolkit for Schools published in 2019, is shown in Appendix B.

Personal data in paper format must be shredded or placed in the confidential waste bins provided. Personal data held in electronic format should be deleted, and CDs and pen drives that hold personal data passed to the I.T. team for safe disposal. Hardware should be appropriately disposed of in compliance with the ICT service provider contract and to ensure conformity with GDPR requirements – this process will be managed onsite by the I.T. Team.

Appendix A is the annual review and statement of compliance with IRMS recommended school retention schedules that is completed by the school. This review has two elements to it, concerning data that is principally managed and held by the school, and that which is the responsibility of the governing body (this is listed in Section 1 of the retention schedule). The review of compliance with all retention dates will be completed by the Data Protection Officer. For data managed by the school the review will involve the Data Protection Officer, Headteacher and the Chair of the Staffing, Staff Wellbeing and Development sub-committee on behalf of the Governing Body. For data managed by the Governing Body, the review will involve the Data Protection Officer, Chair of the Staffing, Staff Wellbeing and Development sub-committee and the Chair of Governors.

9.0 Transferring Personal Data

Any transfer of personal data must be done securely in line with Whitley Bay High School's E-Safety Policy section 9 (outlined above in section 6).

Email communication is not always secure and sending personal data via external email should be avoided unless it is encrypted with a password provided to the recipient by separate means.

Care should be taken to ensure emails containing personal data are not sent to unintended recipients. It is important that emails are addressed correctly and care is taken when using reply all or forwarding or copying others in to emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.

Personal email accounts should not be used to send or receive personal data for work purposes.

10.0 Data Subjects Right of Access (Subject Access Requests)

Under GDPR, individuals (both staff and Pupils) have the right of access to their personal data held by Whitley Bay High School. This applies to data held in both paper and electronic format, and within a relevant filing system.

Whitley Bay High School shall use its discretion under GDPR to encourage informal access at a local level to a data subject's personal information, but it will also have a formal procedure for the processing of Subject Access Requests.

Any individual who wishes to exercise this right should make the request in writing by contacting the Data Protection Officer at Whitley Bay High School (via the general enquiry tab on the 'Contact Us' page of our website).

Whitley Bay High School will not charge a fee. It will only release information upon receipt of a written request along with proof of identity or proof of authorisation where requests are made on the behalf of a data subject by a third party. The requested information will be provided within the statutory timescale of 1 month from receipt of the necessary documentation.

Privacy notices for students, staff, parents and suppliers are all available in the GDPR section of our website, accessible here.

WBHS currently shares student, parent or staff information with external providers in order to facilitate teaching and learning and to ensure the smooth running of the school. A list of all providers is available in the GDPR section of our website (link above).

WBHS also has a charitable Trust which accesses data of those who wish to participate. Information is available in the GDPR section of the school website.

11.0 Reporting a Data Security Breach

It is important Whitley Bay High School responds to a data security breach quickly and effectively. A breach may arise from a theft, a deliberate attack on School systems, and unauthorised use of personal data, accidental loss or equipment failure. Any data breach should be reported to the Data Protection Officer (via the general enquiry tab on the 'Contact Us' page of our website) and if it relates to an IT incident (including information security), should also be reported to the Headteacher.

Any breach will be investigated in line with the procedures within the GDPR. In accordance with that Policy, Whitley Bay High School will treat any breach as a serious issue. Each incident will be investigated and judged on its individual circumstances and addressed accordingly.

The Staffing, Staff Wellbeing and Development Committee will receive an annual report of data breaches in the 2nd meeting of each academic year.

Data breaches that are reportable will be brought to the governors at the first available meeting of the Staffing, Staff Wellbeing and Development Committee. Serious breaches will be reported to the Chair of Governors straight away.

Appendix A: Annual review and statement of compliance with Information and Records Management Society recommended Schools Retention Schedule

Review completed by school
Data Protection Officer: _____

Date: _____

For data held on behalf of the school

Approved by Headteacher: _____

Date: _____

Confirmation from Chair of Staffing, Staff Wellbeing and Development Sub-Committee on behalf of Governing Body of acceptance of Annual review: _____

Date: _____

For data held on behalf of the governing body

Approved by Chair of Staffing, Staff Wellbeing and Development Sub-Committee: _____

Date: _____

Confirmation by Chair of Governing Body: _____

Date: _____

Annual report of Data breaches was presented to the Staffing, Staff Wellbeing and Development Committee

Confirmed by Chair of Staffing, Staff Wellbeing and Development Sub-Committee: _____

Date: _____

Note – The completion of this review will be shared on an annual basis at the second Staffing, Staff Wellbeing and Development Governors meeting of each academic year. A note that the review has been completed and viewed will be added to the minutes.