Prince Henry's Grammar School

COLLABORATIVE LEARNING TRUST

DATA PROTECTION POLICY

1. Introduction

Prince Henry's Grammar School is required to keep and process certain information about its members of staff and students in accordance with its legal obligations under Data Protection Legislation (see section 2), including the General Data Protection Regulation (GDPR).

The school may, from time to time, be required to share personal information about its staff or students with other organisations, as set out in the school's privacy notices (see Appendix C for link to the relevant page of the school website).

This policy is in place to ensure all staff and governors are aware of their responsibilities, and outlines how the school complies with the core principles of Data Protection Legislation.

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

2. Legal framework

This policy has due regard to Data Protection Legislation and other relevant legislation, including, but not limited to, the following:

- The Data Protection Act 2018 (DPA2018)
- The United Kingdom General Data Protection Regulation (UK GDPR)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- 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
- Any legislation implemented in connection with the aforementioned legislation.

Where data is processed by a controller or processor established in the European Union or comprises the data of people in the European Union, it also has regard to the EU General Data Protection Regulation (EU GDPR). This includes any replacement legislation coming into effect from time to time.

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'
- Department for Education (2018) 'Data protection: a toolkit for schools'

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

- Freedom of Information - Publication Scheme
- Computing Facilities Guidance and Acceptable Use Policy
- CCTV Policy

3. Definitions

For the purpose of this policy, ***personal data*** refers to information that relates to an identifiable, living individual. Data Protection Legislation applies to both automated personal data and to manual filing systems.

Sensitive personal data is referred to in Data Protection Legislation as 'special categories of personal data'. This refers to information such as racial or ethnic origin, political opinions, religious or philosophical beliefs, health or disability.

Definitions of other key terms used in the context of this policy are as follows:

- **Data subject** – an individual who is the subject of the personal data (e.g. students, staff).
- **Data controller** – a person or organisation who determines the purposes and ways that data is processed (e.g. Prince Henry's Grammar School).
- **Data processor** – someone who processes data on behalf of the school (e.g. a third-party software provider).
- **Data Protection Officer (DPO)** – the person responsible for ensuring the school is compliant with data protection legislation.
- **Data Lead** - the member of staff responsible for the day-to-day oversight of data processing at Prince Henry's.

4. Principles

In accordance with the requirements outlined in Data Protection Legislation, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by Data Protection Legislation in order to safeguard the rights and freedoms of individuals (e.g. anonymisation).
- 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.

5. Accountability

Prince Henry's Grammar School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in Data Protection Legislation. The school will provide comprehensive, clear and transparent Privacy Notices (See see Appendix C for link to the relevant page of the school website). Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Legal basis for the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Details of recipients of personal data
- Description of technical and organisational security measures

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

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

Data Protection Impact Assessments (DPIAs) will be used, where appropriate.

6. Data Protection Officer (DPO) and Data Lead

A DPO will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with Data Protection Legislation.
- Monitor the school's compliance with Data Protection Legislation, including internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to members of staff, as appropriate.

The Data Protection Officer role at Prince Henry's is fulfilled by a specialist external provider (DPO Centre), in line with most local schools. Our Data Protection Officer (Alison Jones) can be contacted at dpo@princehenrys.co.uk.

Day-to-day oversight of data processing activities will be provided by the school's Data Lead, the Executive Officer: Exams, Data & Curriculum (Michael Stone).

7. Lawful processing

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

Under Data Protection Legislation, data will be lawfully processed under the following conditions:

1. The consent of the data subject has been obtained.
2. Processing is necessary for:
    - 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 school as data controller.
    - For the performance of a contract with the data subject, or to take steps to enter into a contract (e.g. recruitment of staff, Community Education learners).
    - Protecting the vital interests of a data subject or another person.

Sensitive personal data will only be processed under the following conditions:

1. Explicit consent of the data subject, unless reliance on consent is prohibited by law.
2. Processing relates to personal data manifestly made public by the data subject.
3. Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
    - Reasons of substantial public interest on the basis of law which is proportionate to the aim pursued, and which contains appropriate safeguards.

- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of law or a contract with a health professional.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

8. Consent

Where 'consent' is the legal basis upon which data is processed, the following points will apply:

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- Where consent is given, a record will be kept documenting how and when consent was given.
- The school ensures that consent mechanisms meet the standards of Data Protection Legislation. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of current Data Protection Legislation.
- Consent can be withdrawn by the individual at any time.
- Where a child is under the age of 13, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

9. The right to be informed

Privacy notices relating to the processing of the personal data will be written in clear, plain language which is concise, transparent and easily accessible, and will be published on the school website.

The following information will be supplied within the privacy notice:

- The identity and contact details of the controller (i.e. the school) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- Any recipient or categories of recipients of the personal data.
- Details relating to retention periods.
- The existence of the data subject's rights, including the right to:
  - Withdraw consent (where applicable).
  - Lodge a complaint with the Information Commissioner's Office (ICO).

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, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds will be provided. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

10. The right of access

Individuals have the right to obtain confirmation that their data is being processed, as well as the right to submit a data subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

The school's Data Lead (Michael Stone) is responsible for the handling of data subject access requests made to the school. Once received, the Data Lead will investigate and respond to the request accordingly, taking into account the requirements of Data Protection Legislation.

Where a data **subject access request** (SAR) is submitted, the following points will apply:

- The school will verify the identity of the person making the request before any information is supplied.
- 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.
- Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
- Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
- All fees will be based on the administrative cost of providing the information.
- All requests will be acknowledged and processed without undue delay, and a response provided within one month of receipt, at the latest (except where the following points apply).
- In the event of numerous or complex requests, the period of compliance may be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request. It may also be necessary to extend the period of compliance during periods of school closure.
- 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 Information Commissioner's Office (ICO) and to a judicial remedy, within one month of the refusal.
- In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

The school's process for submitting / dealing with a data subject access request is set out in Appendix A.

11. The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification, where possible. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

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

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 Information Commissioner's Office (ICO) and to a judicial remedy.

12. The right to erasure

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

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 (where applicable as a legal basis)
- When the individual objects to the processing and there is no overriding legal basis for continuing the processing
- Where the personal data was unlawfully processed
- Where the personal data is required to be erased in order to comply with a legal obligation

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

- To exercise the right of freedom of expression and information
- To comply with a legal obligation or 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

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. 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.

13. The right to restrict processing

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

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

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

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.

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

14. The right to data portability

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

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

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

The following points will apply in relation to requests for data portability:

- Personal data will be provided in a structured, commonly used and machine-readable form.
- The school will provide the information free of charge.
- Where feasible, data will be transmitted directly to another organisation at the request of the individual. The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.
- 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.
- The school will respond to any requests for portability within one month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.
- Where no action is being taken in response to a request, the 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 Information Commissioner's Office (ICO) and to a judicial remedy.

15. The right to object

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

Individuals have the right to object to the following:

- Processing based on the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task:

- 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.

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.

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.

16. Automated decision-making and profiling

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

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

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

When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Prince Henry's Grammar School understands that automated decisions must not concern a child or be based on the processing of sensitive data, unless:

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

17. Privacy by design and privacy impact assessments

The school will act in accordance with Data Protection Legislation 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. This includes providing appropriate awareness training for staff, including the publication of a 9-point **Data Privacy Checklist** (see Appendix B), which is distributed to staff as part of the induction process, and at the start of each school year.

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. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

High risk processing includes, but is not limited to:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- Changes to, or expansion of, the CCTV system

The school will ensure that all DPIAs include the following information:

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

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 Data Protection Legislation.

18. Data breaches

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.

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

The following procedures will apply in the case of a personal data breach:

- Any personal data breach (or suspected personal data breach) must be reported immediately to the school's Data Lead, Michael Stone, who will seek advice from the Data Protection Officer.
- Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Information Commissioner's Office (ICO) will be informed.
- All notifiable breaches will be reported to the ICO within 72 hours of the school becoming aware of it.
- The risk of the breach having a detrimental effect on the individual, and the need to notify the ICO, will be assessed on a case-by-case basis.
- 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.
- A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the ICO.
- 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 ICO needs to be notified.

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 school's 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

Prince Henry's Grammar School understands that failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

19. Data security protocols

The following specific data security protocols will be implemented to maximise data security:

- Confidential paper records will be kept in a locked filing cabinet or drawer, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Personal data in digital form is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up.
- Where personal data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet or drawer when not in use.
- Memory sticks will not be used to hold personal information unless they are password-protected and encrypted.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- All necessary members of staff are provided with their own secure login and password
- Emails containing sensitive or confidential information are password-protected.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- When sending confidential information by fax, staff will always check that the recipient is correct before sending.
- 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.
- Before sharing data, all staff members will ensure:
  - They are allowed to share it.
  - That adequate security is in place to protect it.
  - That who will receive the data has been outlined in a privacy notice.
- 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.
- The physical security of the school's buildings and storage systems, and access to them, is reviewed regularly. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Prince Henry's Grammar School takes its duties under Data Protection Legislation seriously and any unauthorised disclosure may result in disciplinary action.

20. Data retention

The school's Retention Policy takes account of the retention schedules produced by the Information Record Management Society - http://irms.org.uk/page/SchoolsToolkit

Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable. Some educational records relating to former students 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.

Paper documents will be shredded or disposed of through the use of confidential waste bins. Electronic memories will be scrubbed clean or destroyed, once the data should no longer be retained.

21. Policy review

This policy is reviewed every year. Updated privacy notices are published at the start of each school year.

Appendix A

DATA SUBJECT ACCESS REQUEST: PROCEDURE

Request in Person

Request via Phone

Request via Email

Access to SAR Form

Office Staff print out SAR Form **or** direct to website *www.princehenrys.co.uk* (Our School / School Policies) for Data Subject to download SAR Form

Office Staff direct to website *www.princehenrys.co.uk* (Our School / School Policies) for Data Subject to download SAR Form

Office Staff send email to direct to website *www.princehenrys.co.uk* (Our School / School Policies) for Data Subject to download SAR Form

Complete Application

Data Subject:
Completes form and produces scanned copies of ID

Representative (if required):
Completes form, produces scanned copies of ID and gets authorisation from the Data Subject.

Submit Application

Data Subject emails completed SAR Form to *dpo@princehenrys.co.uk*

Data Subject posts / delivers application to:
Data Protection Officer (SAR)
Prince Henry's Grammar School,
Farnley Lane, Otley LS21 2BB

Office Staff forward application to Data Lead (Executive Officer: Exams, Data and Curriculum)

Data Lead instigates full SAR process:

1. Verifies identity of applicant
2. Sends email acknowledgement to applicant
3. Refers to DPO Centre DSAR guidance doc
4. Considers age-related criteria
5. Consults DPO Centre adviser
6. Contacts relevant staff (e.g. Year Manager, SENCO, Safeguarding Lead)
7. Completes electronic data search
8. Redacts data, if appropriate
9. Prepares response, in consultation with DPO
10. Provides written response to applicant

Appendix B

Prince Henry's
Data Privacy Checklist

1. THINK before you print it

Do you really need a hard copy? This increases the risks to data privacy (especially sensitive data such as PCPs).

2. PRINT it securely

Always use your ID badge to release printing on communal printers.

3. MINIMISE it

Could you colour-code SEN, PP etc in your mark book? Do you need to include surnames on your class profile?

4. SECURE it

Never leave PCPs, mark books etc in classrooms (unless locked away).

5. SHRED it

Never use waste bins to dispose of personal data.

6. LOCK it

Lock your screen when away from your device. Take care to log out properly.

7. PROTECT it

You are responsible for the security of your own devices (eg anti-malware software).

8. ENCRYPT it

Only use encrypted USBs if saving personal data. Always use encrypted documents when emailing sensitive data.

9. Don't SHARE it

Only pass on personal data if you are sure you have the right to. If unsure, check.

Appendix C

Privacy notices

Please see the school website here under **Our School / School Policies** for a copy of the current version of the following documents:

- Privacy notice for students, parents and carers
- Privacy notice for staff
- Privacy notice for Community Education learners