Yardleys School

WORKING TOGETHER FOR A BETTER FUTURE

GDPR POLICY

Adopted by Governors:

Signed: ……

Date: ……June 2020……..……

This policy is reviewed every two years by the Finance, Premises and Staffing Committee

Review date: ……

POLICY INFORMATION

Date of last review	June 2020	Review period	Annual
Date ratified by governors		Governors' committee responsible	Finance, Premises & Staffing
Policy owner	David Pohl	SLT member responsible	David Pohl
Date of next review	June 2022		

Reviews/revisions

Review date	Changes made	By whom
June 2020	Point 10 – Added meetings with Business Manager to discuss any issues Added providing regular updates to governors	David Pohl

Dates of linked staff training (if applicable)

Date	Course title	Led by

EQUALITY AND GDPR

All Yardleys' policies should be read in conjunction with our Equal Opportunities and GDPR policies.

Statement of principle - Equality

We will take all possible steps to ensure that this policy does not discriminate, either directly or indirectly against any individual or group of individuals. When compiling, monitoring and reviewing the policy we will consider the likely impact on the promotion of all aspects of equality as described in the Equality Act 2010.

Statement of principle - GDPR

Yardleys School recognises the serious issues that can occur as a consequence in failing to protect an individual adult's or child's personal and sensitive data. These include emotional distress, physical safety, child protection, loss of assets, fraud and other criminal acts.

Yardleys School is therefore committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA)/GDPR.

1. Our Commitment

Yardleys School recognises the serious issues that can occur as a consequence in failing to protect an individual adult's or child's personal and sensitive data. These include emotional distress, physical safety, child protection, loss of assets, fraud and other criminal acts.

Yardleys School is therefore committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA)/GDPR.
https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

Changes to data protection legislation shall be monitored and implemented in order to remain compliant with all requirements.

The member(s) of staff responsible for data protection is: David Pohl (Data Protection Officer DPO) or in his absence the Headteacher.

The school is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

2. Notification:

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO:
https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified immediately to the individual(s) concerned and the ICO.

3. Personal and Sensitive Data:

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO.

The principles of the GDPR shall be applied to all data processed:

Article 5 of the GDPR requires that personal data shall be:

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

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

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

d) 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;

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

f) 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.

4. Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them.

5. Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO.

Risk and impact assessments are carried out on four types of stakeholder data subjects and the various types of data processing associated with each

i. Pupils
ii. Employees
iii. Governors
iv. Third party e.g. parents, visitors, contractors

Security of data shall be achieved through the implementation of proportionate physical and technical measures. The DPO shall be responsible for the operational effectiveness of the controls implemented and reporting of their performance. These include

a. Cyber security measures for the school IT network
b. Security measures for data used with mobile technology, storage devices or accessed from outside the school
c. Physical storage and disposal of data in school
d. Physical storage of data taken outside of school

The security arrangements of any organisation with which data is shared shall also be considered and these organisations shall provide evidence of their commitment and competence in the security of shared data.

6. Data sharing:

All organisations which provide services which involve the processing of personal data under the Academy's control will be required to sign a data processing agreement. This agreement sets out the terms, requirements and conditions on which the third party will process personal data when providing its services.

7. Photographs and Video:

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.

Staff should only use school equipment and storage rather than using personal devices or taking images out of school.

Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.

It is the school's policy that external parties (including parents & carers) may not capture images of staff or pupils during such activities without prior consent.

8. Data Access Requests (Subject Access Requests):

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:
David Pohl (Data Protection Officer – DPO)
A charge may be applied to process the request if it is considered manifestly unfounded or excessive.

9. Data Retention & Disposal:

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance:
https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

Any source used by the School for the disposal of IT assets and collections will be checked for compliance with ICO guidance.

10. Roles, responsibilities, internal controls and monitoring procedures

The school DPO will: -

- Inform and advise the School, its staff and governors about their obligations to comply with the GDPR and other data protection laws
- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.)
- Update audits on an annual basis and carry out risk assessments (DPIAs) as required
- Maintain a record of any data breaches and subject access requests
- Meet with the Headteacher, Academy Business Manager regularly to discuss any issues, developments, incidents or remedial actions as necessary
- Update governors periodically via the appropriate subcommittee meeting and Headteacher's termly school report
- Train all staff on an annual basis and provide updates and advice as required
- Coordinate and oversee the provision of effective data protection measures

The Academy Business Manager will:-

- Ensure all external suppliers provide written notification of their compliance and protection measures
- Collect all necessary consent from the relevant stakeholders

The Headteacher is: -

- responsible for monitoring the work of the DPO and academy business manager as outlined in this policy

The governing body is:-

- responsible for the GDPR policy and the accountability of the Headteacher

11. Contact, Communication and Complaints

In the first instance all communication regarding data protection/GDPR should be made to:

David Pohl (Data Protection Officer):David.Pohl@yardleys.bham.sch.uk

In his absence contact:

Brynley Evans (Headteacher): Brynley.Evans@yardleys.bham.sch.uk