BRIGSHAW LEARNINGPARTNERSHIP

Data Handling Policy

Approved by BLP Board: April 2020

Adopted by LGB: summer 2020

For publication on school websites

For Review: March 2022

Contents

2. Statement of intent

Brigshaw Learning Partnership (BLP) is required to keep and process certain information about its staff members, volunteers, parents, governors, directors, service providers and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

The school may, from time to time, be required to share personal information with other organisations, such as the LA, Department for Education, other schools and educational bodies, and potentially children's services.

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

Organisational methods for keeping data secure are imperative, and The Brigshaw Learning Partnership recognises that, by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the Academy, and provide evidence for demonstrating performance and accountability.

This document provides the policy framework through which this effective management can be achieved and audited.

This policy complies with the requirements set out in the GDPR and the Data Protection Act 2018

3. Legal framework

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
- Data Protection Act 2018 (DPA)
- The Protection of Freedoms Act 2012 when referring to our use of biometric data.
- DfE Keeping Children Safe in Education Guidance

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- ICO guidance 'Privacy by Design'
- Section 46 FOI Act Code of practice on managing records
- The ICO's code of practice for the use of surveillance cameras and personal information.

This policy will be implemented in conjunction with the following policies, such as but not limited to:

- E-safety Policy
- Freedom of Information Policy
- CCTV Policy (where a school uses CCTV)
- Acceptable e-mail user Policy
- Staff Code of Conduct Policy
- Records Management Retention Schedule

In addition, this policy complies with our Funding Agreement and Articles of Association.

4. Applicable data

This policy applies to all records created, received or maintained by permanent and temporary staff of the BLP in the course of carrying out its functions. Also, by any agents, contractors, consultants or third parties acting on behalf of the school or the multi-academy trust.

Records are defined as all those documents which facilitate the business carried out by the BLP and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronic format, e.g., paper documents, scanned documents, e-mails which document business activities and decisions, audio and video recordings, text messages,

notes of telephone and Skype conversations, spreadsheets, MS Word documents, and presentations.

5. Principles

In accordance with the requirements outlined in the GDPR, 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; 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.

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 the GDPR in order to safeguard the rights and freedoms of individuals.

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.

The Academy will manage and document its records disposal process in line with the Records Retention Schedule. This will help to ensure that it can meet FOI requests and respond to requests to access personal data under data protection legislation (Subject Access Requests, SARS).

The GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the data protection principles”.

6. Accountability

- Brigshaw Learning Partnership will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR and DPA.
- The school will provide comprehensive, clear and transparent privacy policies.
- Additional internal records of the school’s processing activities will be maintained and kept up-to-date.
- Internal records of processing activities will include the following:
    - Name of the organisation
    - Purpose(s) of the processing
    - Description of the categories of individuals and personal data

- Recipients of personal data

- Data Protection Impact Assessments will be used, where appropriate.

- **Staff are accountable for**:
  - Collecting, storing and processing any personal data in accordance with this policy
  - Informing the school of any changes to their personal data, such as a change of address
  - Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not, they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

7. Data protection officer (DPO)

- A DPO will be appointed in order to:
  - Inform and advise the academy trust, school and its employees about their obligations to comply with the GDPR and other data protection laws.
  - Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on Data Protection Impact Assessments, conducting internal audits, and providing support for Headteachers completing the required training to staff members, directors and governors.
  - Serve as the main point of contact and cooperate fully with the supervisory authority (ICO).
  - Provide an annual report of their activities directly to the trust board and, where relevant, report to the board their advice and recommendations on school data protection issues.

- The DPO will report to the highest level of management at the Brigshaw Learning Partnership, the Chief Education Officer.
- The DPO will operate independently and will not be dismissed or penalised for performing their task.

- Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.
- The Data Protection Officer for the Brigshaw Learning Partnership is Wendy Harrington

8. Lawful processing

- The lawful basis for processing data will be identified and documented prior to data being processed.
- Under the GDPR, data will be lawfully processed under the following conditions:

  The consent of the data subject has been obtained or 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 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. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

- Special Category data will only be processed under the following conditions:

  Explicit consent of the data subject, unless reliance on consent is prohibited by ~~EU or~~ UK law.

  Processing carried out 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:

  - 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 defense of legal claims or where courts are acting in their judicial capacity.
  - Reasons of substantial public interest on the basis of UK 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 UK 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 in accordance with Article 89(1).

9. Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

10. Consent

- 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 the GDPR. 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 1998 will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- Consent can be withdrawn by the individual at any time.
- Where a child is under the age identified by the ICO as being able to give consent, the consent of parents will be sought prior to the processing of their data if appropriate, except where the processing is related to preventative or counselling services offered directly to a child. For children over the age of 12, the child's consent will be sought to the processing of their data (where consent is required).

11. The right to be informed

- 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.
- The school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.
- 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.
    - The legitimate interests of the controller or third party.
    - Any recipient or categories of recipients of the personal data.
    - The existence of the data subject's rights, including the right to:
    - Opportunity to withdraw consent at any time.
    - How to lodge a complaint with a supervisory authority.
- 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.
- Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds.
- For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.
- In relation to data that is not obtained directly from the data subject, this information will be supplied:
    - Within one month of having obtained the data.
    - If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
    - If the data are used to communicate with the individual, at the latest, when the first communication takes place.

12. The right of access - Subject Access Requests (SARs)

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request in respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a Subject Access Request.

SARs from parents or carers of pupils who are 12 and above may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

- Individuals have the right to obtain confirmation that their data is being processed.
- Individuals have the right to submit a subject access request (SAR) to gain access to their personal data.
- 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 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 responded to without delay, usually no later than one calendar month, starting from the day the request is received. If the school needs additional information to be able to deal with the request (e.g. ID documents), the time limit will begin once the school have received the additional information requested.
- 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.
- 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.
- 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.

We may not disclose information in a SAR for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it.
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

If staff receive a Subject Access Request in any form, they must immediately forward it to the DPO who will advise on completion.

13. 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 incorrect 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 supervisory authority and to a judicial remedy.

14. 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
    - If the legal basis for processing the data, was consent and 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
- 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
- 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.
- 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.

15. The right to restrict processing

- Individuals have the right to block or suppress the school's processing of personal data unless the school processes the data as part of its legal duties or performing a task in the public interest.
- 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 unless the data is part of legal proceedings.

Where an individual has objected to the processing and the school is considering whether the school's 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.

16. 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
- 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 supervisory authority and to a judicial remedy.

17. 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 legitimate interests or 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 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 defense 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.

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

18. Parental requests to see the educational record

The BLP schools, as academies, are not obliged to provide parents, or those with parental responsibility, access to their child's educational record. However, in most cases the BLP will provide student performance data on request until the pupil concerned is aged over 18.

Access may be denied, if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

19. Biometric recognition systems

Where we use staff or pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012. Note: in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before any biometric data is taken from their child.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). The school will provide alternative means of accessing the relevant services for those pupils/staff members.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

Once an individual leaves the school, biometric data will be destroyed.

20. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers/students aged 18 and over for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school: on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school: by external agencies such as the school photographer, in newspapers and school marketing campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

21. CCTV

- The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
- The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.
- Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
- All CCTV footage will be kept for a maximum of 28 days unless required for an investigation.

Please see BLP CCTV policy for further information.

22. Privacy by design and privacy impact assessments

- The 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.
- 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.
- 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.
- 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.
- A DPIA will be used for more than one project, where necessary.
- High risk processing includes, but is not limited to, the following:
    - 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
    - The use of CCTV.
- 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
    - An assessment and mitigation of risks to children.
- 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.

23. Data breaches

In the event of a suspected data breach, staff will follow the BLP Data Breach Procedure

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 headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.
- Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.
- All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.
- The risk of the breach having a detrimental effect on the rights and freedoms of the individual, and the need to notify the relevant supervisory authority, 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 relevant supervisory authority.
- In the event that a breach is sufficiently serious, the public will be notified without undue delay.
- 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.
- 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
- Failure to report a breach when required to do so may result in a fine to the BLP, as well as a fine for the breach itself.

24. Data security

- Personal Identifiable confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive and regularly backed up.
- Personal memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
- All electronic devices are password-protected to protect the information on the device in case of theft. Passwords are not shared.
- 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/governors are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

- 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 reasonable 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.
    - 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 on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- Brigshaw Learning Partnership takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- Continuity and recovery measures are in place to ensure the security of protected data.
- Personal devises should be password protected and have anti-virus installed.
- Staff and governors are advised to use different passwords for different sites.
- All shredders used to destroy personal information on site are cross - shred.

25. Publication of information

- Brigshaw Learning Partnership publishes on its website:

  Policies and procedures

  Annual reports

  Financial information

  Governance information

  Attainment information.

- Brigshaw Learning Partnership will not publish any personal information, including photos, on its website without the permission of the individual.
- 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.

26. Data retention

- Data will not be kept for longer than is necessary.
- Unrequired data will be deleted/securely destroyed as soon as practicable.

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

27. DBS data

- All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
- Data provided by the DBS will never be duplicated.
- 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.

28. Complaints

An individual wishing to make a complaint about anything relating to this policy should refer to the BLP Complaint Policy published on the BLP Website.

29. Equality Impact Statement

We will do all we can to ensure that this policy does not discriminate, directly or indirectly. We shall do this through regular monitoring and evaluation of our policies. On review we shall assess and consult relevant stakeholders on the likely impact of our policies on the promotion of all aspects of equality, as laid down in the Equality Act (2010). This will include, but not necessarily be limited to: race; gender; sexual orientation; disability; ethnicity; religion; cultural beliefs and pregnancy/maternity.

30. Monitoring and review

Data handling will be formally reviewed in the school to ensure compliance with this policy and the Data Protection Act. Governors and Directors will receive updates on compliance monitoring.

This policy will be reviewed every 2 years.