THE BEWDLEY SCHOOL

We fly with our own wings

THE BEWDLEY SCHOOL

Data Protection & GDPR (General Data Protection Regulation) Policy

Adoption Date: July 2024
Person Responsible: Operations Manager

THE BEWDLEY SCHOOL FOUNDATION
Alis volamus propriis

1. Statement of intent

The Bewdley School is required to keep and process certain information about its staff, students, applicants, parents / carers and contractors in accordance with its legal obligations under data protection legislation including General Data Protection Regulation (GDPR).

The Bewdley School may, from time to time, be required to share personal information about its staff, students, applicants, parents / carers and contractors with other organisations, mainly the LA (Local Authority), other schools and educational bodies, and potentially social services and the police.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the School complies with the following core principles of the GDPR. Organisational methods for keeping data secure are imperative, and The Bewdley School believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in both the Data Protection Act 2018 & GDPR, which came into effect on 25 May 2018.

The School has appointed the following as the DPO (Data Protection Officer): Mr A Whordley (DataProtection@bewdley.worcs.sch.uk)

2. Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018 (DPA).
- School Standards and Framework Act 1998.
- Freedom of Information Act 2000.
- [New] Electronic Commerce (EC Directive) Regulations 2002.
- [New] The Privacy and Electronic Communications (EC Directive) Regulations 2003.
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018).
- Protection of Freedoms Act 2012.

This policy will also have regard to the following guidance:

- Information Commissioners Office ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'.
- Information Commissioners Office ICO (2012) 'IT asset disposal for organisations'
- Department for Education DfE (2018) 'Data protection: a toolkit for schools'.

3. Applicable data

For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

Sensitive personal data is referred to in the UK GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

Processing of sensitive personal information known as 'special categories of personal data' is prohibited unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

The school's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the School can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the school can demonstrate compliance with the GDPR.

The school has implemented measures that meet the principles of data protection by design and data protection by default, such as:

- Minimising the processing of personal data.
- Pseudonymising personal data as much as possible.
- Ensuring transparency in respect of the functions and processing of personal data.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

4. 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 be considered compatible 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 GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

5. Accountability

- The Bewdley School has implemented appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR 2018 & Data Protection Act 2018.
- The Bewdley School will provide comprehensive, clear and transparent privacy policies.
- 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:
  o Name and details of the organization.
  o Purpose(s) of the processing.
  o Description of the categories of individuals and personal data.
  o Retention schedules.
  o Categories of recipients of personal data.
  o Description of technical and organisational security measures.
  o Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

The School will implement measures that meet the principles of data protection by design and data protection by default, such as:
- Data minimisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

Data protection impact assessments will be used, where appropriate.

6. Data protection officer (DPO)

The school has appointed a DPO in order to:

- Inform and advise the Leadership Team about their obligations to comply with the UK 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 the required training to staff members.
- Cooperate with the ICO and act as the first point of contact for the ICO and for individuals whose data is being processed.

The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to Schools. The DPO will report to the highest level of Leadership, which is the Senior Leadership Team. 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.

7. Lawful processing

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

- The consent of the data subject has been obtained.
- Processing is necessary for a contract held with the individual, or because they have asked the school to take specific steps before entering into a contract.
- Processing is necessary for compliance with a legal obligation (not including contractual obligations).
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Processing is necessary for protecting vital interests of a data subject or another person, i.e. to protect someone's life.
- Processing is necessary 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.

The school will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or

former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - 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 with a basis in 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 with a basis in law.
  - 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 a basis in law.
- When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed.
- Why the personal data is being processed.
- What the lawful basis is for that processing.
- Whether the personal data will be shared, and if so, with whom.
- The existence of the data subject's rights in relation to the processing of that personal data.
- The right of the data subject to raise a complaint with the ICO in relation to any processing.

8. Consent

The Bewdley School will ensure that consent is explicit. The School will not use data if based on inferred silence, inactivity or automatic 'opt-in'.

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 is collected as required under 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.

The Bewdley School recognises that from their thirteenth birthday students are freely able to make the informed decision around consent of the processing of their data. The Bewdley School will not seek to obtain consent at the age of thirteen years, but accept consent can be withdrawn by the individual at any time.

The consent of the parent will be sought prior to the students thirteenth birthday for legal processing of the child's data, except where the processing is related to preventative or legal services offered or directly effecting the child. e.g. LAC (looked after child).

Where the school opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined above.

9. 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.

If services are offered directly to a student, the School will ensure that the privacy notice is written in a clear, plain manner that the student will understand.
In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information is provided 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:
  o Withdraw consent at any time.
  o Lodge a complaint.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

10. The right of access

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 in order to verify the lawfulness of the processing.
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. 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 responded to without delay and at the latest, within one month of receipt. 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.

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 supervisory authority and to a judicial remedy.

12. The right to removal

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 (if this is possible).
- 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 personal data is processed in relation to the offer of information society services to a child.

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 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 student 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 student 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.

13. The right to restrict processing

Individuals have the right to block or suppress the School 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.

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 Bewdley 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.

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 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 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 may from time to time send information to parents, students, staff or other stakeholders if the school believes this information to be pertinent or of interest. The individual can at any time refuse or opt-out of these communications. At no time will The Bewdley School use personal details for third party marketing, to sell or push a product.
- The Bewdley School accepts no liability, nor endorses any product, service or company for the purposes of marketing to parents, students, staff or other stakeholder.

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 an 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.

16. Privacy by design and privacy impact assessments / measures

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 audits will be used to identify the most effective method of complying with the School's data protection obligations and meeting individuals' expectations of privacy.

Data audits 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 Bewdley School's reputation which might otherwise occur. When using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, or where high-risk data processing is identified. The School will consult the ICO (Information Commissioners Office) to seek its opinion as to whether the processing operation complies with the GDPR.

17. 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 Headteacher will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development 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.

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.

All notifiable breaches will be reported to the ICO authority 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 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.

The School recognises failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

18. Data Security

- 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 that is regularly backed up off-site.
- Where data is saved on removable storage or a portable device, the device will be encrypted or kept in a locked filing cabinet, drawer or safe when not in use.
- 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.
- Where possible, the School enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff and governors will not use their personal laptops or computers to store personal (student or staff) School related data on at any time, unless the device is encrypted or school property.
- All necessary members of staff 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 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 they are responsible for the security of the data while in their possession and will follow guidance as set out within this policy.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- The recipient 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 termly basis. If an increased risk in vandalism / burglary / theft is identified, extra measures to secure data storage will be put in place.

- The Bewdley School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- The Data Protection Officer (DPO) is responsible for continuity and recovery measures are in place to ensure the security of protected data.

19. Safeguarding

The school understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

The school will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared.
- What data was shared.
- With whom data was shared.
- For what reason data was shared.
- Where a decision has been made not to seek consent from the data subject or their parent.
- The reason that consent has not been sought, where appropriate.

The school will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk. The school will

manage all instances of data sharing for the purposes of keeping a child safe in line with the Safeguarding Policy.

20. Publication of Information

Copies of information that The Bewdley School may publish can be found within the privacy notice found on the School website. Information that could be published include, but not exclusively:

- Policies and Procedures.
- Annual Reports (to an individual/individual's parents).
- Termly Reports (to an individual/individual's parents).
- Social Media Stories.
- New Stories on Website.
- News Stories on App.
- Publications within local or national newspapers.

21. CCTV and Photography

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 students, staff and visitors of the purpose for collecting CCTV images via signs, a notice in reception and the Schools CCTV policy.

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 three months for security purposes; the Data Protection Officer is responsible for keeping the records secure and allowing access. The School will always indicate its intentions for taking photographs of students and will retrieve permission before publishing them. If the School wishes to use images / video footage of students in a publication, such as the School website, prospectus, or recordings of school performances, written permission will be sought for the particular usage from the parent of the student or student (if over the age of 13).

Images captured by individuals for recreational / personal purposes, and videos made by parents for family use, are exempt from the UK GDPR. The Bewdley School accepts no liability or responsibility for images or video footage being recorded by a third party and then shared while on the premises. The Bewdley School will ensure everyone is aware of their responsibilities, but are not responsible for their actions forthwith.

Parents / carers and others attending school events are able to take photographs and videos of those events as long as they are for domestic purposes only. Photographs or videos being used for any other purpose are prohibited to be taken by parents or visitors to the school.

22. Data Storage including Cloud

For the purposes of this policy, 'cloud' refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the school accessing a shared pool of ICT services remotely via a private network or the internet.

All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the school.

All files and personal data will be encrypted before they leave a school device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. As with files on school devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the school should unauthorised access, deletion or modification occur, and ensure ongoing compliance with the school's policies for the use of cloud computing.

The school's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

23. Data Retention

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 pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

All data is retained for as long as is outlined within the School's Data Retention Policy.

24. DBS Data

All data provided by the DBS (Disclosure Baring service) 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.

25. Staff Appointment / Exit and Training

The Bewdley School as part of its recruitment and exit interview process for employees ensure that staff are aware of their responsibilities. As part of staff induction, staff are made aware of their responsibilities under GDPR.
When a member of staff leaves employment at The Bewdley School, the School ensure that no data relating to the school or an individual is removed with that member of staff. Staff receive regular training as part of their continuous professional development around Data Protection issues, processes and procedures. This is provided through

input from the schools DPO in whole staff training, access to online CPD modules through the schools training provider and regular updates during the year.

26. Requesting access to personal data

Under General Data Protection Regulation, parents / carers and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to educational record, contact DataRequest@bewdley.worcs.sch.uk

Appendix:

Appendix 1 – Breach of Personal Data Procedure
Appendix 2 – Guidance / Advice on school principles on GDPR

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost.
    - Stolen.
    - Destroyed.
    - Altered.
    - Disclosed or made available where it should not have been.
    - Made available to unauthorised people.
- The DPO will alert the CEO in the first instance.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Examples of actions relevant to specific data types are set out at the end of this procedure).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will advise on whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

    - Loss of control over their data.
    - Discrimination.
    - Identify theft or fraud.
    - Financial loss.
    - Unauthorised reversal of pseudonymisation (for example, key-coding).
    - Damage to reputation.
    - Loss of confidentiality.

- Any other significant economic or social disadvantage to the individual(s) concerned.

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out a description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned.
- The categories and approximate number of personal data records.
- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause.
  - Effects.
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Records of all breaches will be kept in accordance with regulation.

- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach. Full guidance is given to staff as part of their induction to each Academy and is reissued annually.

Appendix 2: Guidance / Advice on school principles on GDPR

The Bewdley School GDPR Protocols and Guidance for Staff, agency, supply and visitors.

The Bewdley School takes the storage and protection of personal data very seriously, and is governed by the GDPR (General Data Protection Regulation) 2018 and Data Protection Act 2018. The Bewdley School have the following guidance to ensure data is safeguarded and the risk on individuals handling data is minimised.

Staff, agency, supply and visitors should make every effort to follow the guidance and protocols highlighted below. There may be occasions where the guidance below is not applicable or circumstances require a different action to be taken. In these situations, staff, agency, supply and visitors should inform a Senior member of staff at their earliest opportunity.

The guidance below has been designed to ensure that privacy and the rights of the individual and the data are protected. While The Bewdley School recognises that all risk cannot be removed, staff, agency, supply and visitors should make every effort to ensure that these guidelines are followed to the best of their capability.

What is Data?

In context of GDPR the following forms of data are characterised as protected/private data. That the school, staff, agency, supply and visitors should ensure is secure.

- Name
- Address
- Phone Number
- Date of Birth
- Place of Birth
- Unique ID Number (UPN, exam number)
- Medical
- Workplace or School
- Email Address
- IP Address
- Social media account name
- Sexual orientation
- Reviews
- SEN

Emails:

When communicating any personal information, only school email accounts can be used. Personal email access is not allowed as highlighted in the schools AUP (Acceptable Usage Policy).

- Emails containing data should only be sent to email addresses that are known and trusted organisation e.g. not @gmail.com. The owner of the email account must be confirmed before any information is sent.
- If data is being shared, permissions must be sought and authorised that the data sharing is allowed.
- Do not send any personal details in the body of an email to someone outside of school.

- If information is sent outside of school, data should be put in a document and password protect this file. (*To encrypt a document, create the document, go to File, Info, Protect Document, Encrypt with Password.)*
- Do not send the password to open the file in the same email, either phone and / or email the password separately.
- Do not put the name of a person in the subject bar.
- When reference students in an email use the student's first name and initial of surname e.g. Ben S Year 10.
- Before forwarding an email, ensure that any personal information is removed from the previous emails e.g. names, email address.
- Do not reply all to a personal email, only reply to the required individuals.
- Passwords should be complex (numbers and letters) and must not be used for private accounts as well.
- Only access emails on a personal device, ensuring that no-one is around that could read or take any of the data.
- Do not send emails to multiple recipients in the 'To:' field, emails should be sent using the 'BCC' field so email addresses are not shared.

Mobile Phones:

- If School emails are set up on personal mobile phones or devices, devices should be password encrypted to gain access.
- When email access is granted to a mobile device, the School has the power to wipe the device if lost or stolen. In the event of a theft or loss staff must inform the school at their earliest opportunity.
- Ensure that automatic sign in to emails is not setup on devices where they are shared with other members of the family.

USB Memory Sticks/USB External Hard Drives:

- The Bewdley School allows the use of personal Memory Sticks and External Hard Drives for storage and transport of documents.
- Only non-sensitive data can be stored and transported on USB devices. e.g. lesson plans, resources, videos (not of students).
- If a USB storage device needs to carry personal data, then either the document and / or the device itself must be encrypted (password protected).
- Devices must not be left unattended, plugged into computers or lying around.
- USB storage devices must only be used on computers that have up to date anti-virus software installed on them.

Coursework/Exercise Books:

- Coursework and Exercise books should be kept in classrooms in boxes when not in the possession of the student.
- In the case of taking coursework / exercise books home for marking / moderating purposes, the top document should be placed face down to cover any names.
- Coursework / exercise books should be taken from school straight to home addresses and stored indoors overnight and not left in vehicles unattended.

Displays / Notice boards:

- Consent must be obtained for any names, photos or work to be placed on display.
- Ensure that the environment in which documents are being displayed is considered to ensure no private data is shared with non-school members.

Interactive Whiteboards:

- Do not display SIMS, tracking sheets, medical information or emails on classroom projectors. Ensure the projector is turned off, or screens are 'frozen' before accessing such data.

GDPR Consent:

An up-to-date list of GDPR consent for students can be found on the 'Staff Share' in a folder called GDPR.