Data Protection Policy

Incorporating GDPR (general data protection regulation, EU regulation - 2016/679)

Background

Bigland Green Primary School is 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, 1998 (DPA, 1998). The school will comply with DPA and any subsequent relevant legislation (for example, GDPR, May 2018), to ensure personal data is treated in a manner that is lawful and fair. The implementation of the GDPR will be carefully monitored to ensure effective, and demonstrable compliance. This policy should be read in conjunction with the school's Internet Use and other relevant policies.

Registration and dealing with any breaches

The school's data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. 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 within 72 hours to the individual(s) concerned and the ICO.

Data gathering

All personal data relating to staff, pupils or other people with whom the school has contact, whether held on computer or in paper files, are covered by the Act. Only relevant personal data may be collected and the person from whom it is collected will be informed of the data's intended use and any possible disclosures of the information that may be made. The legal bases for processing data are as follows:

Consent: the member of staff/pupil/parent has given clear consent for the school to process their personal data for a specific purpose.

Contract: the processing is necessary for the staff employment contract or pupil admissions to the school.

Legal obligation: the processing is necessary for the school to comply with the law (not including contractual obligations)

All staff must treat all personal information in a confidential manner and follow this policy. The school is committed to ensuring that its staff are aware of data protection requirements and adequate training is provided to them through appropriate briefing meetings and email notifications. 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.

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 principles of the Data Protection Act shall be applied to all data processed:

1. ensure that data is fairly and lawfully processed
2. process data only for limited purposes
3. ensure that all data processed is adequate, relevant and not excessive
4. ensure that data processed is accurate
5. not keep data longer than is necessary
6. process the data in accordance with the data subject's rights
7. ensure that data is secure
8. ensure that data is not transferred to other countries without adequate protection

Fair processing and/or privacy notice

The school will 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.

There may be circumstances where the school is required either by law or in the best interests of our pupils or staff to pass information onto external authorities, for example local authorities, Ofsted, or the department of health. 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. Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition;
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child, and;
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed.

Data security and storage

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance. The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data. All personal data will be stored in a secure and safe manner.

Electronic data will be protected by standard password and firewall systems operated by the school. Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting either in the office or at the reception hatch. Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data. Particular attention will be paid to the need for security of sensitive personal data.

Location of information and data:

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This is stored with the school office in an appropriate manner but not locked.

Sensitive or personal information and data should not be removed from the school site without the permission of the Headteacher. However, the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils. The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

1. paper copies of data or personal information should not be taken off the school site as they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances;
2. any unwanted data/information must be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name;
3. care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers;
4. if information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended;
5. if it is necessary to transport data away from the school, it should be downloaded onto a storage device. The data should not be transferred from this device onto any home or public computers;

6. storage device that staff use must be encrypted and/or password protected.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Emailing of personal data

Personal data must not be emailed to anyone unless the email used is secure. Organisations using London Grid for Learning (LGfL) have access to USO-FX which is secure. This facility is available to all staff and governors at Bigland Green. Staff LGfL work emails are also secure and can be used for sharing sensitive data when there is a need. Alternatively, 'Egress' can be used as a form of secure email. Please see the computing technician if you need advice or help.

Data Checking

The school will issue regular reminders to staff and parents who are responsible to ensure that personal data held is up-to-date and accurate. Any errors discovered would be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

Data Disclosures

Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given. When requests to disclose personal data are received by telephone it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.

If a personal request is made for personal data to be disclosed it is again the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.

Personal data will not be used in newsletters, websites or other media without the consent of the data subject. Routine consent issues will be incorporated into the school's starter pack, to avoid the need for frequent, similar requests for consent being made by the school.

Personal data will only be disclosed to Police Officers if they are able to supply a written request or a WA170 form which notifies of a specific, legitimate need to have access to specific personal data. A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- **Other schools** - If a pupil transfers from Bigland Green to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.
- **Examination authorities** - This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies. This also includes registration for the 'Artsmark Awards' and other similar projects.
- **Educational division** - Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

- **Health authorities** - As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.
- **Police and courts** - If a situation arises where a criminal investigation is being carried out the school may need to forward information on to the police to aid their investigation. The school will pass information onto courts as and when it is ordered.
- **Social workers and support agencies** - In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.
- **Right to be Forgotten** - Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

Subject access requests

If the school receives a written request from a data subject to see any or all personal data that the school holds about them this should be treated as a Subject Access Request and the school will respond within the 40 day deadline. Informal requests to view or have copies or personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the 40 day time limit.

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. 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) may not capture images of staff or pupils during such activities without prior consent. Personal information and/or images must not be uploaded onto social media sites without written consent from the Headteacher.

Data 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 – please see appendix A.

The school physically destroys IT assets before approved disposal. All sensitive data which is no longer required is shredded and then disposed of in an appropriate manner.

Monitoring of the policy

The school has an internal Data Protection Officer (DPO), and a designated member of the governing body responsible for data protection. They, with the support of the Headteacher, are responsible for monitoring the implementation of this policy. They will also review and advise the Headteacher if an external DPO is necessary.

Date approved	Signature	Review
May 2022		May 2024

Appendix A:

Bigland Green School will ensure that any personal data is not stored for longer than required. The table below shows the length of time for which data may be kept.

	Information	**Length of time for which the information be kept**
Current pupils & parents	Personal details on the school's MIS[1] system	For the length of time that the pupil is at school + six years
	Information kept in the pupil's individual folder (e.g. proof of address, identity, significant communication between home/school and other agencies	For the time that the pupil is at school and then passed on to the next school. If the information cannot be passed on to the next school, then it will be destroyed after six months.
	Raw data gathered for different surveys and/or consultations	Six months
Current employees	Personal information on file	For the length that they are employed by the school + six years
	Working time records Appraisal records	Two years from the date the records refer to
	Payroll records Maternity, paternity and pay	Three years after the end of the tax year that the payment stopped
Former staff	Personnel folder	Six years from the date of the resignation or termination of employment
Other	Application received from prospective candidates	Three months from the closing date of the application
	Application and other documentation for short-listed candidates who are not appointed	Six months from the closing date of the application
	Visitors on 'Visited'	All printed data to be destroyed after 12 months.

[1] MIS – Management Information System