Forest Sports Education
Data Protection & GDPR Policy
Date of Review: September 2025

Date of Next Review: September 2026

Signed, Richard Kear (Managing Director):

Contents Page

Data Protection Policy
General Data Protection Regulation
The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

This document meets the requirement at paragraph 1 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.

It also meets the requirement at paragraph 5 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018 and company intends to rely on these as and when appropriate, with particular reliance on paragraph 18, 'Safeguarding of children and individuals at risk' and paragraph 17, 'Counselling'.

1. Introduction
In order to work effectively, Forest Sports Education has to collect and use information about people with whom it works. This may include (past, present and future) pupils, parents, teachers, members of the public, contractors and suppliers. In addition, we may be required by law to collect and use information in order to comply with the requirements of the central government.

All personal information must be handled and dealt with properly, regardless of how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by other means. We are all responsible for its safe handling.
This document sets out the principles of data protection, our responsibilities, and the access rights of individuals, as well as information sharing and complaints.

2. Scope/ Our Commitment
This policy applies to all staff, contractors, agents, representatives and temporary staff, working for or on behalf of Forest Sports Education. The requirements of this policy are mandatory for all of these parties.

Forest Sports Education regards the lawful and correct treatment of personal information as critical to its successful operation, maintaining confidence between the company and those it interacts with. The company will ensure that it treats personal information correctly in accordance with the law.

Forest Sports Education fully endorses and adheres to the principles of Data Protection as set out in the Data Protection Act (2018) and the General Data Protection Regulation (GDPR).

Forest Sports Education is committed to ensuring that their staff are aware of data protection policies, legal requirements and that adequate training is provided.

Changes to data protection legislation, under the GDPR and DPA, shall be monitored and implemented in order to remain compliant with all requirements.

3. Principles of Data Protection
The GDPR outlines seven key principles for anyone who processes personal data. These principles form the basis of our approach to processing personal data.

Guide to data protection | ICO
Key definitions of the Data Protection Act | ICO

• ensure that data is fairly and lawfully processed
• process data only for limited purposes
• ensure that all data processed is adequate, relevant and not excessive
• ensure that data processed is accurate
• ensure that data is not kept for longer than is necessary
• process the data in accordance with the data subject's rights
• ensure that data is secure
• ensure that data is not transferred to other countries without adequate protection.

4. Responsibilities
Data breaches shall be notified within 72 hours to the individual(s) concerned.
The members of staff responsible for data protection within the School are mainly the managing director (Richard Kear) and the general managers (Josh Carter & Jack Fowler). However all staff must treat all pupil (or other relevant) information in a confidential manner and follow the guidelines set out in this document.

5. Definitions of Data

Personal data is information about living, identifiable individuals. It covers both facts and opinions about the individual but need not be sensitive information. The GDPR makes a distinction between personal data and “special category” (sensitive) data. Special category personal data requires stricter conditions for
Processing.

Personal data is defined in s(1) of the GDPR, as ‘data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of the data controller’ (the School is a data controller), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual.

Special Category Data is information about racial or ethnic origin, sexual life or sexual orientation, biometric and genetic data, religious beliefs (or similar), physical or mental health/condition, membership of a trade union, political opinions or beliefs, details of proceedings in connection with an offence or an alleged offence.

6. Processing Personal Data

We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law. When special category personal data, criminal conviction data or data about offences, is processed, a lawful basis and additional condition will be satisfied.

- The data needs to be processed so that the company can fulfil a contract with the individual, or the individual has asked the company to take specific steps before entering into a contract.
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone’s life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the company or a third party (provided the individual’s rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

7. Fair Processing / Privacy Notice

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

8. Sharing Data

There may be circumstances where the company is required either by law or in the best interests of our pupils or staff to pass information on to external authorities, for example local authorities, Ofsted, or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect. Any proposed change to the processing of an individual's data shall first be notified to them. 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:

- Health authorities

As obliged under health legislation, the company may pass on information regarding the health of children in the company 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, we may have to forward information on to the police to aid their investigation. We will pass information on to courts as and when it is ordered.

- Social workers and support agencies

In order to protect or maintain the welfare of our pupils in our care, and in cases of suspected child abuse, it may be necessary to pass personal data on to social workers or support agencies.

9. Photographs and Videos

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

We will obtain written consent from parents/carers for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental

consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Images used on inschool magazines, brochures, prospectuses newsletters, etc.
- Online on our company website or social media pages/ feeds.
- 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.

10. Data Protection Rights of the Individual

Data Access Requests (Subject Access Requests)

All individuals, whose data is held by us, have a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

Richard Kear, Forest Sports Education, Kings Buildings, Lydney, Gloucestershire, GL15 5HE

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)
- Where 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

11. Data Security

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

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 their competence in the security of shared data.

12. Location of Information and Data

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard or office. The only exception to this is medical information that may require immediate access during the day. This will be stored in the head office. Sensitive or personal information and data should not be removed from the head office. However, the company acknowledges that some staff may need to transport data between the schools the company works at and their home in order to access it for work.. 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:

- Paper copies of data or personal information should not be taken away from head office. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data away from head office, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- 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.

- Due to the nature of the business, all staff are required to use google drive. All documents used should be google documents (or GSheets/ GSlides) and these should be saved on the company's google drive.
- In order to protect staff and others, staff are not allowed to download or save any documents to their personal computer or USB.
- In addition, staff should also use a company email address which is provided. Any communication with other parties should take place via their company email. Personal email addresses should not be used. When emailing other parties, all staff should carbon copy a member of senior management (Richard Kear, Josh Carter, Jack Fowler).

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.

13. Data Disposal

The company 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.

14. Complaints

Complaints about how the company processes data under the GDPR and responses to subject access requests are dealt with using the company's complaints procedure.

15. Breach of Policy

Any breach of this policy should be investigated in accordance with our Data Breach process. The company will always treat any data breach as a serious issue, potentially warranting a disciplinary investigation. Each incident will be investigated and judged on its individual circumstances, addressed accordingly and carried out in line with the employee code of conduct.