



Forest Sports Education

Document Safety Policy

Date of Review: September 2025

Date of Next Review: September 2026

Signed, Richard Kear (Managing Director):

1. Introduction

In order to work safely and effectively, ProStars will need to produce and use documents which need to be shared with the company. For example, ProStars staff will need to produce lesson plans which may need to be shared with ProStars and other stakeholders (e.g. schools).

This policy has been produced to protect all staff involved in working for ProStars. It outlines strict policies and procedures which must be adhered to by all staff.

2. Use of documents

Any documents produced and used for ProStars behalf must be done so using the business Microsoft domain prostars-fse.com. For example, the following documents must be saved on the company Sharepoint.

These documents must be used so that they can be saved in a central location. All documents produced and used on ProStars behalf must be created using one of the 3 platforms above (apart from promotional materials where Kami can be used). Once these documents have been created they must be uploaded to the shared drive.

3. Saving documents

When saving documents, they must be saved to the shared drive. Staff must not save company documents on their personal laptops. If any staff member is found to save company documents on their own personal laptops disciplinary action will be taken. This is to allow transparency in all matters relating to the company. Documents must be saved in appropriate folders.

4. Safeguarding

When referring to issues regarding safeguarding, these documents must be saved in the safeguarding folder within the shared drive. This folder restricts access so only those that need to see it, will see it. It also protects staff members and the company as all documents relating to incidents are shared in a central location.

5. 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 sharepoint. All documents used should be Microsoft documents and these should be saved on the company's sharepoint.
- 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.