Data Retention Policy

The Green Room Foundation is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

GDPR requires data minimisation and data protection by design and default (Article 25) – meaning data controllers and processors must implement appropriate technical and organisational measures, such as a ‘blurring technique’ (pseudonymisation), which are designed to implement data-protection principles, such as data minimisation.

Owner: NA/**W**AA/**K**LF/**6**NA

Date Created	Date 1st Review Due	Date Reviewed	Version	Next Review Due
May 2018	May 2019	May 2019	2	May 2020
		October 2020	3	October 2021
		February 2021	4	February 2022
		February 2022	5	February 2023
		February 2023	6	February 2024
		January 2024	7	January 2025
		January 2025		January 2026
		January 2026		January 2027

1. Introduction

The emphasis under the UK GDPR is data minimisation both in terms of the volume of data stored on individuals and how long it is retained for.

To summarise the legal requirements, Article 5 (e) of the UK GDPR states that personal data shall be kept for no longer than is necessary for the purposes for which it is being processed. There are some circumstances where personal data may be stored for longer periods (eg data relating to SEN or child protection or medical incidents).

Recital 39 of the UK GDPR states that the period for which the personal data is stored should be limited to a strict minimum and that time limits should be established by the data controller for deletion of the records (referred to as erasure in the UK GDPR) or for a periodic review.

In the course of providing an education, The Green Room creates and holds records of student, parent/carer and employee information. The Green Room demonstrates public accountability through the proper retention and disposal of records, and that decisions are taken with proper authority and in accordance with due process. Records are kept in the Accountability Documentation Record.

2. Aims and Objectives

The purpose of this policy is to set out the length of time that The Green Room's records should be retained and the processes for disposing of records at the end of the retention period.

3. Scope

The policy covers the categories of data listed in the Data Retention Schedule irrespective of the media on which they are created or held including:

- Paper;
- Electronic files (including Arbor, or Google documents)
- Spreadsheets,
- E-mails
- Photographs, videos

The Schedule aims to include all types of categories of records which The Green Room creates or holds. They include:

- Admissions
- Attainment
- Attendance
- Behaviour
- Exclusions
- Identity Management (photos on documents)

- Trips and Activities
- Medical Info and Administration
- Safeguarding
- SEN
- Personal identifiers, contacts and personal characteristics

4. Data Subject Rights and Data Integrity

1. **A Right of Subject Access -** A data subject has a right to be supplied by The Green Room with the personal data held about him or her.
2. **A Right of Correction -** A data subject may force The Green Room to correct any mistakes in the data held about them.
3. **The right to object or restrict processing** - A data subject may object to, or request restriction of, the processing of their personal data where this is permitted under UK GDPR.
4. **A Right to Prevent Direct Marketing -** A data subject may stop their data being used in attempts to sell them things (eg by junk mail or cold calling.)
5. **A Right to Prevent Automatic Decisions -** A data subject may specify that they do not want a data user to make "automated" decisions about them
6. **A Right of Complaint to the Information Commissioner -** A data subject can ask for the use of their personal data to be reviewed by the Information Commissioner who can enforce a ruling using the DPA. The Commissioner may inspect a controller's computers to help in the investigation.
7. **A Right to Compensation -** The data subject is entitled to use the law to get compensation for damage caused ("damages") if personal data about them is inaccurate, lost, or disclosed.

5. Technical and Organisational Data Security Measures

Student, parent/carer and staff data is held in our system - Arbor Education.
Each user is issued with a unique and secure password, with permission-based access ensuring that they can only view the data relevant to them. No data is stored on any device, and Arbor automatically logs out after a period of inactivity. Arbor uses bank-grade, end-to-end, 256bit SSL encryption to ensure only we can see our data. Student data is NEVER shared with third parties without The Green Room Foundations' consent.
Emails, photos, the website, apps and all provision documents are stored in our G Suite for Education which is UK GDPR compliant. All data not in these two systems is kept in a locked cupboard in The Green Room office, access to which is through a locked door.
Where records are stored using cloud-based systems, retention and deletion are managed in accordance with contractual agreements and data protection safeguards to ensure compliance with UK GDPR.

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely. Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.
- Staff should note that unauthorised disclosure and/or failure to adhere to the requirements set out below will usually be a disciplinary matter, and may be considered gross misconduct in some cases.
- Personal information should be kept in a locked cupboard or in a locked drawer; or if it is computerised, be password protected; or when kept or in transit on portable media the files themselves must be password protected.
- Personal data should never be stored at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the Head of Provision must be obtained, and all the security guidelines given in this document must still be followed.
- Data stored on portable electronic devices or removable media is the responsibility of the individual member of staff who operates the equipment. It is the responsibility of this individual to ensure that: Suitable backups of the data exist; Sensitive data is appropriately encrypted; Sensitive data is not copied onto portable storage devices without first consulting the data protection officer in regard to appropriate encryption and protection measures. Electronic devices such as laptops, mobile devices and computer media (USB devices, CD's etc) that contain sensitive data ARE not left unattended when offsite.
- For some information the risks of failure to provide adequate security may be so high that it should never be taken home. This might include payroll information, addresses of students and staff, disciplinary or appraisal records or bank account details. Exceptions to this may only be with the explicit agreement of the Head of Provision.

6. Data Disposal

A data audit is carried out in the last month of the provision year. Data is removed in accordance with our Data Retention Schedule. All records containing personal information, or sensitive policy information should be made either unreadable or unreconstructable.

• Paper records should be shredded
• CDs / DVDs / Floppy Disks should be cut into pieces
• Hard Disks should be dismantled and sanded
• Electronic files should be deleted

Where records are destroyed internally, the process must ensure that all records are authorised to be destroyed by a member of the Leadership team and the destruction recorded. Records should be shredded as soon as the record has been documented as being destroyed

The data destroyed is recorded in the Data Destruction Checklist

7. Data Retention

A recommended minimum retention period is provided for each category of record in the Data Retention Schedule and works in conjunction with Arbor's Data Retention Policy which is as follows:

The minimum retention period is the greater of
(a) 6 years after the student's leaving date from the provision, or
(b) if relating to a child, the 24th birthday of the child, or
(c) if relating to more than one child, the 24th birthday of the youngest child.

(Not all records are retained until a student's 24th birthday; shorter retention periods apply where there is no safeguarding, legal, or statutory requirement to retain the information.)

Retention periods are determined by statutory requirements, safeguarding considerations, limitation periods for potential legal claims, and operational needs.

The lawful bases most commonly relied upon for retaining records are public task, legal obligation, and vital interests, particularly in relation to safeguarding, welfare, and health and safety.

The following records should be stored separately to the student record as they are subject to shorter retention periods and if they are placed in Arbor then it will involve a lot of unnecessary weeding of the files.

• Absence notes
• Parental consent forms for trips/outings [in the event of a major incident all the parental consent forms should be retained with the incident report not in the student record]
• Correspondence with parents about minor issues
• Accident forms (these are stored separately and retained in The Green Room office until their retention period is reached. A copy could be placed on the student file in the event of a major incident)

E-mails

E-mail that needs to be kept should be identified by content; for example, does it form part of a student record? Is it part of a contract? The retention for keeping these e-mails will then correspond with the classes of records according to content in the retention schedule. These e-mails may need to be saved into Arbor or printed out and placed on paper files

This policy should be used in conjunction with the Data Retention Schedule.

This policy is approved by the CEO of The Green Room Foundation

Date:

CEO: