Data Protection 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.

The public good is in nothing more essentially interested, than in the protection of every individual's private rights - Blackstone

The General Data Protection Regulation (GDPR) / Data Protection Act 2018 has been considered in the drafting of this policy. Being an alternative educational provision - The Green Room School needs to collect data and information and also use that data and information. Personal data is typically gathered from pupils, parents/carers and staff but can include others associated with The Green Room School. The purpose of data collection is always to aid the betterment of the school and subsequently the pupils themselves. Data will never be gathered unnecessarily. Data collection is a legal issue and The Green Room School will be required to comply with said legal guidelines.

The Green Room School is registered with the Information Commissioner's Office. The following policy outlines The Green Room Foundation's approach to Data Protection.

Date Created	Date 1st Review Due	Date Reviewed	Version	Next Review Due
March 2014	March 2015	April 2015	2	April 2016
		October 2016	3	October 2017
		October 2017	4	April 2018
		May 2018	5	May 2019
		May 2019	6	May 2020
		September 2020	7	September 2021

Purpose

This policy establishes an effective, acceptable and transparent framework for ensuring compliance with the requirements of the GDPR.

Personal information needs to be handled securely and correctly, it is the purpose of this policy to ensure that. This policy applies to any and all data collected by The Green Room and ultimately will aid the learning of pupils and allow staff to monitor and report on pupil progress.

Scope

This policy applies to all The Green Room School employees and all third parties responsible for the processing of personal data on behalf of The Green Room Foundation.

The Rights of Data Subjects

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure (some of these rights are not going to apply due to other conditions set out in the Lawful Basis Section)
- the right to restrict processing
- the right to data portability
- the right to object
- rights in relation to automated decision making and profiling.

4. The Data Protection Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations.
Article 5 of the GDPR requires that personal data shall be:
“a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) 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 not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) 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;
e) 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; and
f) 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."
Article 5(2) requires that:
"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Lawful, Fair, and Transparent Data Processing

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means The Green Room School must tell the data subject what processing will occur, (transparency) the processing must match the description given to the data subject (fairness) and must be for one of the purposes specified in the applicable data protection regulation (lawfulness)

The Green Room obtains consent from pupils who are over 18 and parents to process their data for the specific purposes of: providing education to the pupil and safeguarding. Please see appendix A for consent letter and privacy policy.

Our 6th Form premises is based in a school room and technical suite at The Swan Pub in Clewer which uses CCTV throughout the public areas. Green Room pupils need to access the school through areas which are covered by CCTV, and participate in activites in public areas covered by CCTV, for example in the courtyard and the pub. The school room and technical suite DO NOT have CCTV. Please see The Swan CIC Data Protection Policy and CCTV policy.

Specified, Explicit, and Legitimate Purposes

Personal data must only be collected for specified explicit and legitimate purposes and not further processed in a way incompatible with those purposes. This means The Green Room School must specify exactly what the personal data collected is for and limit the processing of that personal data to only what is necessary to meet the specific need.

Adequate, Relevant, and Limited Data Processing

Personal data shall be adequate, relevant and limited only in relation to the purposes for which they are processed. This means The Green Room School will not store any personal data beyond strictly required (see Data Retention Schedule)

Accuracy of Data and Keeping Data Up-to-Date

Personal data must be accurate and kept up to date. This means The Green Room School will identify and address out of date, incorrect and redundant personal data. This will take

place in a yearly audit in the last month of the school year. Personal data shall be kept in a form which enables identity of the data subject for no longer than necessary for the purpose for which the data was originally needed. This means The Green Room must wherever possible store personal data which limits or prevents identification of the data subject.

Data Retention

Please see Data Retention Policy and Data Retention Schedule

Secure Processing

Personal data shall be processed in a manner that ensures appropriate security of data, including protection against unauthorised or unlawful processing and against accidental loss or damage. The Green Room uses appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all time. All data is stored either in Arbor Education or Google G-Suite for education.

Accountability and Record-Keeping

The Data Controller shall be responsible for and be able to demonstrate compliance. This means The Green Room School must demonstrate how the data protection principles outlined above apply to the personal data for which it is responsible. Please see Accountability Documentation below which is stored in a GDPR folder on the Google Drive

Data Protection Impact Assessments

Please see Data Protection Impact Assessment Policy and DPIA Template

Keeping Data Subjects Informed

Please see Privacy Policy - Pupils and Parents / Workforce

Data Subject Access

Please see Subject Access Request Policy and Subject Access Request Form

Rectification of Personal Data

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing but preferably via the Data Rectification Form. The Green Room will respond within one calendar month to the request.
In certain circumstances we have the right to refuse a request for rectification. This right is closely linked to the controller's obligations under the accuracy principle of the GDPR (Article (5)(1)(d)).

Erasure of Personal Data

Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

When does the right to erasure apply?

- Individuals have the right to have their personal data erased if:
- the personal data is no longer necessary for the purpose which The Green Room originally collected or processed it for;
- The Green Room is relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;
- The Green Room is relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- The Green Room is processing the personal data for direct marketing purposes and the individual objects to that processing;
- The Green Room has processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- The Green Room has to do it to comply with a legal obligation; or
- The Green Room has processed the personal data to offer information society services to a child.

An individual can make a request for the right to erasure verbally or in writing but preferably via the Data Erasure Form

When does the right to erasure not apply?

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

Restriction of Personal Data Processing

Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

When does the right to restrict processing apply?

Individuals have the right to request you restrict the processing of their personal data in the

following circumstances:

- the individual contests the accuracy of their personal data and The Green Room is verifying the accuracy of the data;
- the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- The Green Room no longer needs the personal data but the individual needs The Green Room to keep it in order to establish, exercise or defend a legal claim;
- the individual has objected to The Green Room processing their data under Article 21(1), and we are considering whether our legitimate grounds override those of the individual.

How do we restrict personal data?

The Green Room will temporarily restrict the record in Arbor, preventing users from accessing it. Images can be removed from the website and accounts can be suspended in Google.

When can we lift the restriction?

Once The Green Room has made a decision on the accuracy of the data, or whether our legitimate grounds override those of the individual, we may decide to lift the restriction. However, the individual must be informed before we lift the restriction.

Making a request

An individual can make a request for restriction verbally or in writing, preferably by the Data Restriction form. The Green Room will respond to such a request within one month.

NOTE: the right to erasure or restriction - whilst an individual is employed by or attending The Green Room, there may be data that we would not erase or restrict if requested if it would hamper our ability to perform our public task

Data Portability

The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that The Green Room transmits this data directly to another school / college.

When does the right apply?

The right to data portability only applies when:

- the lawful basis for processing this information is consent or for the performance of a contract;
- we are carrying out the processing by automated means (ie excluding paper files).

What does the right apply to?

Information is only within the scope of the right to data portability if it is personal data of the individual that they have provided to The Green Room.

The right to data portability entitles an individual to:

•receive a copy of their personal data;
•have their personal data transmitted from one controller to another controller.

An individual should make the request in writing, preferably via the Data Portability Request form. The Green Room will respond within one month.

The Green Room will:

The Green Room will provide from Arbor a Common Transfer File (CTF) to provide data to another controller or will provide a Data Collection Sheet in a pdf format to the individual.

Objections to Data Processing

Article 21 of the GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask The Green Room to stop processing their personal data.

The right to object only applies in certain circumstances. Whether it applies depends on The Green Room's purposes for processing and our lawful basis for processing. An individual can ask The Green Room to stop processing their personal data for direct marketing purposes at any time. This is an absolute right and there are no exemptions or grounds for refusal.

The Green Room obtains consent from individuals to process their data for the specific purposes of either providing an education or a place of employment and for safeguarding purposes and to object to the processing of personal data would hamper our ability to perform our public task.

Personal Data Collected, Held, and Processed

Please see Privacy Policy Workforce and Privacy Policy Pupil/Parent

Data Security

Article 5(1)(f) of the GDPR concerns the 'integrity and confidentiality' of personal data. It says that personal data shall be:

'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'

Storage

Pupil, 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. Pupil data is NEVER shared with third parties without The Green Room schools' consent.

Emails, photos, the website, apps and all school documents are stored in our G Suite for Education which is GDPR compliant. All data not in these two systems is kept in a locked cupboard in school office, access to which is through a locked door.

For CCTV data please see the Swan CIC Data protection policy.

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. Ordinarily, personal data should not be processed 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 School 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 pupils and staff, disciplinary or appraisal records or bank account details. Exceptions to this may only be with the explicit agreement of the Head of School.

Disposal

A data audit is carried out in the last month of the school 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

Please also read The Green Room School Security Policy

Data Breach Notification

Please see Data Breach Policy and Data Breach Log

Implementation of Policy

The Head of school and the Data Protection Officer will ensure that all Green Room employees responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition they will ensure all third parties engaged to process personal data on behalf of The Green Room are aware of and comply with the contents of this policy. Assurance of which must be obtained from all third parties prior to granting access to the personal data controlled by The Green Room School.

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

Date: _____

Co-CEO: _____