Data Protection Policy

Policy Number	31
Organisation	YGAM
Policy owner	Director of Compliance & QA
Date Agreed by Board	6 December 2022
Review Date	December 2025 (3 years from sign off)

1. Scope

The Young Gamers and Gamblers' Education Trust (hereafter referred to as YGAM) and its management and Board of Trustees are committed to being fully compliant with all applicable UK and EU data protection legislation in respect of personal data, as well to safeguarding the "rights and freedoms" of persons whose information YGAM collects pursuant to the Data Protection Act 2018 and the implementation into UK law of the General Data Protection Regulation (EU) 2016/679 (UK GDPR).

This policy applies to all employees of YGAM including contractors and subcontractors. Breaches of this policy shall be dealt with according to YGAM's Disciplinary Policy. If there is a possibility that the breach could amount to a criminal offence, the matter shall be referred to the relevant authorities.

All third parties working with or for YGAM who have or may have access to personal data are required to read, understand, and fully comply with this policy at all times. All third parties are required to enter into a data confidentiality agreement prior to accessing any personal data. The data protection obligations imposed by the confidentiality agreement shall be equally onerous as those to which YGAM has agreed to comply with. YGAM shall always have the right to audit any personal data accessed by third parties pursuant to the confidentiality agreement.

2. Good Practice

YGAM shall ensure compliance with data protection legislation and good practice, by always:

- processing personal information only when to do so is necessary for organisational purposes;
- ensuring that the least possible amount of personal data is collected, and that personal data is never processed unduly;
- informing individuals of how their personal data is or will be used and by whom;
- processing only pertinent and adequate personal data;
- processing personal data in a lawful and fair manner;
- keeping a record of the various categories of personal data processed;
- ensuring that all personal data that is kept is accurate and up to date;
    - retaining personal data no longer than required by statute or regulatory body, or for organisational purposes;
- giving individuals the right of 'subject access', as well as all other individual rights pertaining to their personal data;
- ensuring that all personal data is maintained securely;
- transferring personal data outside of the UK or EEA only in situations where it shall be appropriately secured and only where such transfers comply with the UK GDPR; and
- applying various statutory exemptions, where appropriate.

3. Data Protection Lead

The lead for data protection activities within YGAM is the Director of Compliance & QA.

YGAM's Director of Compliance & QA is:

Caroline Gallagher
dataprotection@ygam.org

The Director of Compliance & QA:

- is accountable for compliance with the requirements of the UK GDPR and the DPA and demonstration of good practice protocol;
- reports to YGAM's Board of Trustees and, amongst other things, is accountable for the development, implementation, and day-to-day compliance with this policy (and all other data protection policies);
- is directly responsible for ensuring that YGAM is UK GDPR and DPA compliant and that managers and executive officers of YGAM are compliant in respect of data processing that occurs within their field of responsibility and/or oversight.

The Director of Compliance & QA is the first point of contact for any employees of YGAM who require guidance in relation to any aspect of data protection compliance.

4. Legal status, registration and records

YGAM is a data controller under Article 4(7) of the UK GDPR for most of its processing activity.

YGAM has therefore registered with the Information Commissioner (under registration number **ZA125536)** as a 'data controller' that engages in processing personal information of data subjects.

YGAM is also a data processor under Article 4(8) of the UK GDPR.

YGAM has identified the personal data that it processes and recorded it in its Record of Processing Activity (ROPA). The ROPA can be found in the QMS. YGAM has separate sections for its data controller and data processor activities.

5. Communication with ICO

The Director of Compliance & QA shall retain a copy of all notifications made by YGAM to the Information Commissioner's Office ("ICO") on the Non-Conformity Log which shall be used as a record of all notifications made.

The ICO notification shall be reviewed on an annual basis in consultation with the CEO and Board of Trustees and the Director of Compliance & QA shall be responsible for each annual review of the details of the notification, keeping in mind any changes to YGAM's activities. These changes shall be ascertained by reviewing the Record of Processing Activities and the management review. Data protection impact assessments shall be used to ascertain any additional relevant requirements.

6. UK GDPR background

The purpose of the UK GDPR is to ensure the "rights and freedoms" of living individuals.

7. Definitions (as per the UK GDPR)

- *Child* means anyone under the age of 18.

- *Data controller* may be a natural or legal person, whether a public authority, agency, or other body which, individually or jointly with others, oversees ascertaining the purposes and means by which personal data shall be processed. Where EU or Member State law predetermines the purposes and means of processing personal data, the data controller or, if appropriate, the specific criteria for selecting the data controller, may be provided for by EU or Member State law.

- *Data subject* refers to any living person who is the subject of personal data (see above for the definition of 'personal data') held by an organisation. A data subject must be identifiable by name, ID, address, online identifier, or other factors such as physical, physiological, genetic, mental, economic, or social.

- *Data subject consent* refers to any specific indication by the data subject that signifies consent to the processing of personal data. Consent may take place by way of a written or oral statement or by clear, unambiguous action and must be given freely at all times, without duress, with the data subject being properly informed.

- *Establishment* refers to the administrative head office of the 'data controller' in the EU, where the main decisions regarding the purpose of its data processing activities are made. 'Data controllers' based outside of the EU are required to appoint a representative within the jurisdiction in which they operate to act on its behalf and liaise with the relevant regulatory and supervisory authorities.

- *Filing system* refers to any personal data set which is accessible based on certain benchmarks, or norms and can be centralised, decentralised or dispersed across various locations.

- *Personal data* – Personal data here refers to data defined under Article 4 of the UK GDPR, which is:

    - any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person

- *Personal data breach* refers to a security breach which results in the disclosure, alteration, destruction, or loss of personal data, as well as unauthorised access to personal data that is stored, transmitted or processed by any other means, whether accidentally or unlawfully.

- *Processing* refers to any action taken in relation to personal data, including but not limited to collection, adaptation or alteration, recording, storage, retrieval, consultation, use, disclosure, dissemination, combination, or deletion, whether by automated means or otherwise.

- *Profiling* refers to any form of personal data processing that is automated, with the intention of assessing personal aspects of a data subject or analysing a data subject's employment performance, economic status, whereabouts, health, personal preferences, and behaviour. The data subject has a right to object to profiling and a right to be informed of the fact that profiling is taking place, as well as the intended outcome(s) of the profiling.

- *Special categories of personal data* refers to personal data which is more sensitive and includes personal data relating to racial or ethnic origin, beliefs - whether religious, political, or philosophical - membership of a trade-union and data relating to genetics, biometric identification, health, sexual orientation and sex life.

- *Third party* is a natural or legal person other than the data subject who is authorised to process personal data, whether a public authority, agency, or other body controller, processor, or any other person(s) under the direct authority of the controller or processor.

8. Responsibilities

In addition to the specific responsibilities assigned to the Director of Compliance & QA in section 3 above, all YGAM employees are responsible for ensuring compliance with data protection laws (See section 20 - Training)

9. Principles of data protection

YGAM will comply with its obligations to act in accordance with the principles of data protection enumerated in Article 5 of the UK GDPR.

The principles of personal data processing are as follows:

1. All personal data must be processed lawfully, fairly and in a transparent manner in relation to individuals. This is the **principle of lawfulness, fairness, and transparency**.
2. All personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This is the **principle of purpose limitation**.
3. Personal data must be adequate, relevant, and restricted to only what is required for processing. This is the **principle of data minimisation**.
4. Personal data must be accurate and up to date. This is the **principle of accuracy**.
5. Personal data must be 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. This is the **principle of storage limitation**.
6. Personal data must 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. This is the **principle of integrity and confidentiality**.
7. The controller shall be responsible for, and be able to demonstrate compliance with, points 1-6 above. This is the **principle of accountability**.

Under the accountability principle, the YGAM is responsible both for ensuring overall compliance with the UK GDPR and for demonstrating that each of its processes is compliant with the UK GDPR requirements. To this extent YGAM is required to:

- Maintain all relevant documentation regarding its processes and operations;
- Implement proportionate security measures;
- Carry out Data Processing Impact Assessments (“DPIAs”);
- Comply with prior notification requirements;
- Seek the approval of relevant regulatory bodies; and
- Appoint a Data Protection Officer if required. (See section 18)

10. Data transfer

Wherever possible YGAM adopts a policy of not transferring personal data outside of the UK or EEA. This means that third parties being considered as data processors for YGAM will generally be excluded if they transfer outside of the UK or EEA.

For the avoidance of doubt 'transferred' means storing, hosting, or accessing personal in or from countries outside of the UK and EEA.

However, should such data transfers be unavoidable, this will only be done if one or more (as appropriate) of the following safeguards are in place:

- Affected data subject have consented to the data transfer;
- The country receiving the transfer provides appropriate protection of the data subject's 'rights and freedoms' in relation to the processing of personal data;
- The transfer occurs within a contractual arrangement that includes appropriate standard contractual clauses; and/or
- Other arrangements are in place to ensure the rights and freedoms of data subjects are protected.

YGAM does work with third parties based outside of the UK or EEA. However, in these cases YGAM generally does not transfer personal data out of the UK or EEA; it trequires that such clients host the personal data exclusively in the UK and EEA. Where this is not possible, YGAM will only agree to work with such third parties where they can ensure and we can ensure that we comply with requirements in the UK GDPR relating to international transfers.

11. The rights of data subjects

In relation to personal data that is processed and recorded, data subjects enjoy the right to:

- make access requests in respect of personal data that is held and disclosed;
- refuse personal data processing, when to do so is likely to result in damage or distress;
- refuse personal data processing when it is for direct marketing purposes;
- be informed about the functioning of any decision-making processes that are automated which are likely to have a significant effect on the data subject;
- not be solely subjected to any automated decision-making process;
- claim damages should they suffer any loss because of a breach of the provisions of the UK GDPR;
- take appropriate action in respect of the following: the rectification, blocking and erasure; of personal data, as well as the destruction of any inaccurate personal data;
- request that the ICO carry out an assessment as to whether any of the provisions of the UK GDPR have been breached;

- be provided with personal data in a format that is structured, commonly used, and machine-readable;
- request that his or her personal data is sent to another data controller; and
- refuse automated profiling without prior approval.

12. Complaints

All complaints about YGAM's processing of personal data may be lodged by a data subject directly with the Director of Compliance & QA by using the complaints procedure. Data subjects can access this complaints procedure by emailing dataprotection@ygam.org.

Complaints may also be made by a data subject directly to the relevant regulatory body and YGAM hereby provides the relevant contact details for the UK regulatory body, the ICO (*https://ico.org.uk/concerns/*).

All queries in relation to how a complaint has been handled, and any appeals following the submission of a complaint, shall be dealt with by the Director of Compliance & Quality Assurance. Please contact at dataprotection@ygam.org.

13. Legal basis

In storing and processing personal data, YGAM generally relies on four lawful bases

- Data Subject Consent (UK GDPR, Art. 6 (1) (a))
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter a contract (UK GDPR, Art. 6 (1) (b))
- Legal obligation (UK GDPR Art. 6 (1) (c))
- Legitimate Interest (UK GDPR, Art. 6 (1) (f))

Whenever YGAM conducts data processing it will identify an appropriate lawful basis for processing and conduct the appropriate documentation or implementation activities. This generally means

- where consent is used a compliant consent mechanism is put in place and
- wherever legitimate interest is used a legitimate interest assessment will be conducted.

In addition, if YGAM processes special category data then it will identify an appropriate condition for processing, as required under Article 9 of the UK GDPR. The available conditions are:

a. Explicit consent;
b. Employment, social security, and social protection (if authorised by law);
c. Vital interests;

d. Not-for-profit bodies;
e. Made public by the data subject;
f. Legal claims or judicial acts;
g. Reasons of substantial public interest (with a basis in law);
h. Health or social care (with a basis in law);
i. Public health (with a basis in law);
j. Archiving, research, and statistics (with a basis in law).

If YGAM relies on conditions (b), (h), (i) or (j), it also need to meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018.

If YGAM relies on the substantial public interest condition in Article 9(2)(g), it also needs to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018.

Where we rely on consent to process the personal data of a child, it is our policy to require the consent of the child's parent or legal guardian where the child is under the age of 12.

14. Data Security

All employees of YGAM are personally responsible for keeping secure any personal data held by YGAM for which they are responsible. Under no circumstances may any personal data be disclosed to any third party unless YGAM has provided express authorisation and has entered into a confidentiality agreement with the third party. Employees are advised to consult with the Director of Compliance & QA before disclosing any personal data to anyone outside of YGAM.

All employees are required to have read and signed the Security Information Policy (DP3) during their staff induction before being granted access to any personal information.

15. Data access rights

Data subjects have the right to access all personal data in relation to them held by YGAM, whether as manual records or electronic format. Data subjects therefore may at any time request to have sight of confidential personal references held by YGAM as well as any personal data received by YGAM from third parties. To do so, a data subject must submit a Subject Information Request, using the Subject Information Request Form (DP7).

This policy covers all personal data that is processed by YGAM.

This policy commits YGAM to:

- fulfil its obligations under Article 15 of the UK GDPR, Rights of Access by the Data Subject for all data processing activities where YGAM is a data controller; and

- fulfil its contractual obligations in respect of requests made to data controllers under Article 15 of the GDPR, for which YGAM acts as a data processor.

Personal data and data subject are defined in Section 7.

As a controller

Under Article 15 of the UK GDPR, where YGAM is a data controller, a data subject is entitled to the following:

1. To obtain from YGAM confirmation as to whether personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
    a. the purposes of the processing;
    b. the categories of personal data concerned;
    c. the recipients or categories of recipient to whom the personal data have been or will be disclosed, particularly recipients in third countries or international organisations;
    d. where possible, the envisaged period for which the personal data will be stored (the retention period), or, if not possible, the criteria used to determine that period;
    e. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
    f. the right to lodge a complaint with the Commissioner;
    g. where the personal data are not collected from the data subject, any available information as to their source;
2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 of the GDPR relating to the transfer;
3. YGAM shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, YGAM may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

As a processor

Where YGAM acts as a data processor for a third-party data controller, it will undertake the following activities:

1. If YGAM receives an access request under Article 15 of the GDPR, it will forward that request to the relevant data controller as soon as possible and in any event no later than 5 days after receiving the request.

2. Where instructed by a relevant data controller following an Article 15 request (whether made directly to the data controller or to YGAM and then passed to the controller), YGAM will provide relevant personal data to the controller.

The Director of Compliance & Quality Assurance shall be responsible for the application and functionality of the procedure associated with this policy and shall handle all Subject Information Requests ("SIRs"). Process can be found in YGAM QMS

16. Disclosure of data

YGAM must take appropriate steps to ensure that no personal data is disclosed to unauthorised third parties. This includes friends and family members of the data subject, governmental bodies and, in special circumstances, even the Police. All employees of YGAM are required to attend specific training to learn how to exercise due caution when requested to disclose personal data to a third party.

Disclosure is permitted by the UK GDPR without the consent of the data subject under certain circumstances, namely in the interests of:

- safeguarding national security;
- crime prevention and detection which includes the apprehension and prosecution of offenders;
- assessing or collecting a tax duty;
- discharging various regulatory functions, including health and safety;
- preventing serious harm occurring to a third party; and
- protecting the vital interests of the data subject i.e. only in a life and death situation.

The Director of Compliance & QA is responsible for handling all requests for the provision of data for these reasons and authorisation by the Director of Compliance & QA shall only be granted with support of appropriate documentation.

Sometimes YGAM shares personal data with third parties. Some of these third parties will be data controllers and other will be data processors for YGAM.

YGAM shall only engage with third party data processors that are able to provide adequate security, including technical, physical, or organisational security, to all personal data that they process on YGAM's behalf.

17. Data retention and disposal

YGAM only retains and processes collected personal data for as long as required, in accordance with the storage limitation principle. The retention period for personal data is dependent on the purpose for which the data was collected and/or applicable law.

YGAM is committed to fulfil its obligations under Article 5(1)(e) of the UK GDPR, the Storage Limitation Principle, which says that personal data shall be:

> "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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')"

YGAM commits to fulfilling the actions governed by the policy and described in the associated procedure.

- **As a controller**

Where YGAM is a data controller of personal data, it will set data retention and deletion requirements for itself and for any third parties that process data for it.

- **As a processor**

Where YGAM is a data processor of personal data under a contract with a third party-data controller, YGAM will seek direction from the data controller about data retention/deletion requirements to be applied to the relevant personal data. YGAM will also implement those requirements in respect of that data.

Personal data must be disposed of according to YGAM's secure disposal procedure, to ensure that the "rights and freedoms" of data subjects it always protected

18. Data Breach

This policy commits YGAM to fulfil its obligations under Article 33 of the UK GDPR, Notification of a personal data breach to the supervisory authority, and Article 34 of the UK GDPR, Communication of a personal data breach to the data subject. Process for reporting and actioning a Data Breach is available in the QMS.

19. Data Protection Officer

Under Article 37 of the UK GDPR, a data controller or processor must appoint a Data Protection Officer (DPO) where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

YGAM believes that none of these criteria apply to it and therefore has decided that it will not appoint a DPO.

20. Data Protection Training

Data protection training is a risk control. YGAM therefore commits to data protection training as follows:

- All new employees will undergo data protection training as part of their induction
- All YGAM employees will undergo data protection training on an annual basis
- Trustees – when they are appointed to the Board and annual refresher.

It is expected that any contractors that supply services for YGAM will have completed sufficient GDPR training.

21. Privacy Impact Assessment

This policy commits YGAM to fulfil its obligations under Article 35 of the UK GDPR, Data Protection Impact Assessment (DPIA).

YGAM commits to operate the following DPIA process:

- Conducting an initial threshold assessment to determine if a mandatory DPIA is required; and
- Completing a mandatory DPIA if required based on the threshold assessment; and
- Any other DPIAs that YGAM may voluntarily decide to complete; and
- Any DPIAs that YGAM may be asked to complete by a third party if YGAM determines that it is within its interest or obligation to do; and
- Any other associated risk documentation such as legitimate interest assessments where legitimate interest is used as a lawful basis for processing.

YGAM will align as much as possible with guidance from the UK data protection regulatory, the Information Commissioners Office, on how to conduct a DPIA.

YGAM commits to conducting DPIAs with sufficient lead time until the ‘go live’ date so that risks identified can be mitigated where possible, risk decisions can be made, and supporting documentation is complete, before going live.

The Director of Compliance & Quality Assurance shall be responsible for the application and functionality of the procedure for DPIAs and shall handle all DPIAs. Process can be found in YGAM QMS.

22. Review

A formal review of this policy will take place every 3 years unless there is a notable change in relevant legislation or business need which triggers a review before that time.