EEG - Data Protection Policy			
Current Status	Live – Awaiting Committee Approval	**Last Review:**	
Responsibility for Review:	Group Director of Compliance & GDPR	**Next Review:**	December 2025
Roles Responsible for Review:	Group GDPR and Compliance Lead	**Originated:**	December 2023
Approved by:	SET Resources	**Committee:**	Audit and Risk Committee
Type of Policy:	Staff	**Quality Assured by:**	

Contents

1. Introduction

1.1 Eastern Education Group (EEG) is committed to protecting the rights and freedoms of data subjects (natural persons), the safe and secure processing of their data, in accordance with the United Kingdom General Data Protection Regulation (UK GDPR) and Data Protection Act 2018. This policy applies to all staff and any other personnel associated with EEG (at each relevant College including West Suffolk College, Abbeygate Sixth Form and One Sixth Form).

1.2 We hold personal data about our employees, students, parents, governance members, suppliers, and other individuals for a variety of purposes.

1.3 This policy sets out how we seek to protect personal data and ensure that our employees understand the rules governing the use of the Personal Data to which they have access in the course of their work.

1.4 EEG leadership is fully committed to ensuring continued and effective implementation of this policy, and expects all employees share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

2. Scope

2.1 This policy applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means (i.e. paper records) that form part of filing system or are intended to form part of a filing system. This applies to all staff, who must be familiar with this policy and comply with its terms.

2.2 This policy supplements our other policies relating to Internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be uploaded into Insight - Single-Sign-On - Select Provider (insight4grc.com).

2.3 The Chief People Officer has overall responsibility for EEG for day-to-day implementation of this policy.

3. Data Controllers and Processors

3.1 UK GDPR applies to data 'Controllers' and 'Processors'.

- A Controller determines the purposes and means of processing personal data.
- A Processor is responsible for processing personal data on behalf of a Controller.

3.2 EEG is a Controller of data and we have specific legal obligations placed upon us; e.g. we are required to maintain records of personal data and processing activities such as employee personnel records and as such we have a legal liability to protect this information and will be held responsible for a breach.

3.3 As a Controller, we are not relieved of our obligations where the Processor is involved (i.e. in a sub contract arrangement EEG is the Controller, the Sub Contractor is the Processor) as UK GDPR places further obligations on us to ensure our contracts with Processors comply with UK GDPR.

4 Types of Data

4.1 UK GDPR applies to Personal Data and Sensitive Personal Data.

5 Personal Data

5.1 Personal Data means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier known as Personally Identifiable Information.

5.2 This definition provides for a wide range of personal identifiers to constitute personal data including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

5.3 Personal data that has been pseudonymised, e.g. key coded, can fall within the scope of the UK GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

5.4 Any information relating to a person that can be used to directly or indirectly identify that person may include their:

- Full name, email address, date of birth, IP address/website cookies
- Purchases, downloads, subscriptions and services used
- Questions and responses, promotions used, survey responses
- Financial history, banking/credit, payment transactions and donations
- Healthcare and education service used
- CCTV recordings, gender identity, location data, credit card data
- Judgements/sanctions, government services

And information that is capable of identifying an individual either on its own or when combined with other information such as

- Internal account numbers, PINs and Passwords, International Mobile Equipment Identity (IMEIs), National Insurance number
- Driving license number, passport number

6 Sensitive Personal Data

6.1 The UK GDPR refers to sensitive data as Special Category Data which is prohibited without explicit consent or specific conditions.

6.2 The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

6.3 Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

6.4 Special Category Data may include:

- Race/Ethnic origin
- Political opinions
- Religious beliefs
- Union Membership
- Biometric, genetic, health/medical data
- Sexual orientation, sex life (including close personal relationships with staff/students)
- Criminal offences
- Criminal convictions

7 Six Principles of GDPR

7.1 EEG shall comply with the principles of data protection (the Principles) enumerated in the UK GDPR. We will make every effort possible in everything we do to comply with these principles. The Principles are:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

b) If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

c) Only processed for 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;

d) Limited to what is relevant and necessary for the purposes for which they are processed;

e) Kept up to date and accurate or rectified; 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;

f) Kept only if required and for no longer than necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods in so far as the personal data will be processes 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 UK GDPR in order to safeguard the rights and freedoms of individuals; and

g) Kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

8 Accountability

8.1 EEG must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. We are responsible for keeping a written record of how all the data processing activities we are responsible for comply with each of the Principles. This must be kept up to date and must be approved by the Group GDPR and Compliance Lead.

8.2 To comply with data protection laws and the accountability and transparency Principle of UK GDPR, we must demonstrate compliance. We are responsible for understanding our particular responsibilities to ensure we meet the following data protection obligations:

a) Fully implement all appropriate technical and organisational measures

b) Maintain up to date and relevant documentation on all processing activities

c) Conducting Data Protection Impact Assessments

d) Implement measures to ensure privacy by design and default, including:

- Data minimisation
- Pseudonymisation
- Transparency
- Allowing individuals to monitor processing
- Creating and improving security and enhanced privacy procedures on an ongoing basis

9 The Six Lawful Basis for Processing

9.1 As a Controller EEG is responsible for, and must be able to demonstrate, compliance with the principles and therefore we must have a valid lawful basis in order to process personal data.

9.2 There are six available bases for processing. No single basis is 'better' or more important than the others. Which basis is most appropriate to use will depend on the purpose and relationship with the individual.

9.3 If you are making an assessment of the lawful basis, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means.

9.4 Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

9.5 Consider the following factors and document your answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

9.6 Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

9.7 We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

9.8 If you are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the Group GDPR and Compliance Lead.

9.9 The six lawful basis for processing are:

a) **Consent:** the individual has given clear consent for the Trust to process their personal data for a specific purpose.

b) **Contract:** the processing is necessary for a contract that EEG has with the individual, or because they have asked us to take specific steps before entering into a contract.

c) **Legal Obligation:** the processing is necessary for EEG to comply with the law (not including contractual obligations).

d) **Vital Interests:** the processing is necessary to protect someone's life.

e) **Public Task:** the processing is necessary for EEG to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

f) **Legitimate interests:** the processing is necessary for EEG legitimate interests or the legitimate interests of a third party, unless there is good reason to protect the individual's personal data which overrides those.

9.9 EEG holds a record of which basis we are relying on for each processing purpose so it is important that the Group GDPR and Compliance Lead and Chief People Officer are aware if a new system for processing data is being introduced to the activities of EEG so that the lawful basis for processing can be determined and documented.

10 Consent

10.1 The UK GDPR sets a high standard for consent. If consent is difficult, then EEG will look for a different lawful basis for processing.

10.2 Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement and enhance EEG's reputation.

10.3 Consent requires a positive opt-in and pre-ticked boxes, or any other method of default consent is not used by EEG.

10.4 Explicit consent requires very clear and specific statements of consent.

10.5 Consent requests are separate from other terms and conditions of EEG and separate consent for separate things/activities are used.

10.6 Where third party controllers are active EEG will name them in the request for consent.

10.7 EEG makes it easy for people to withdraw consent by telling them how they can do this usually in the form of the option to 'opt-out' or by clicking an unsubscribe link.

10.8 Consent to processing is never a precondition of a service provided by the Trust.

11 Contract

11.1 EEG can rely on this lawful basis if we need to process someone's personal data:

a) To fulfil a contractual obligation placed upon us; or

b) Because EEG has been asked to do something before entering into a contract (e.g. to provide a quote).

11.2 Any decision to rely on contract lawful basis will be documented so that justification of the reasoning can be supplied.

12 Legal Obligation

12.1 EEG can rely on this lawful basis if we need to process the personal data to comply with common law or a statutory obligation. This does not apply to contractual obligations.

12.2 The processing must be necessary so if we can reasonably comply without processing the personal data, then this basis will not apply.

12.3 Any decision to rely on this lawful basis will be documented so that justification of the reasoning can be supplied. We will seek to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out our obligation in order to use this lawful basis for processing.

13 Vital Interests

13.1 EEG is likely to rely on vital interests as its lawful basis if we need to process the personal data to protect someone's life.

13.2 EEG will not rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.

13.3 Vital interests are intended to cover only interests that are essential for someone's life. So this lawful basis is very limited in its scope, and generally would only apply to matters of life and death. It is likely to be particularly relevant for emergency medical care, when there may be a need to process personal data for medical purposes and the individual is incapable of giving consent to the processing (i.e. they are unconscious).

13.4 Any decision therefore to rely on this lawful basis is likely to only be for this reason and will be documented so that justification of the emergency medical reasoning can be supplied.

14 Public Task

14.1 EEG can rely on this lawful basis if we need to process personal data in the exercise of official authority. This covers public functions and powers that are set out in law; or to perform a specific task in the public interest that is set out in law.

14.2 This lawful basis is most relevant to public authorities, but it can be applied to any organisation that exercises official authority to carry out tasks in the public interest.

14.3 EEG does not need a specific statutory power to process personal data, but our underlying task, function or power must have a clear basis in law.

14.4 The processing of data under this lawful basis must be necessary so if EEG can reasonably perform the task or exercise our powers in a less intrusive way then this lawful basis will not apply.

15 Legitimate Interests

15.1 Legitimate interests is the most flexible lawful basis for processing, but EEG does not assume it will always be the most appropriate.

15.2 It is likely to be the most appropriate where we use people's data in ways that they would reasonably expect it to be used and which will have a minimal privacy impact, or where there is a compelling justification for the processing.

15.3 There are three elements to the legitimate interest basis. The three part test involves:

1. Identifying the legitimate interest;
2. Showing that the processing is necessary to achieve it; and
3. Balancing it against the individual's interests, rights and freedoms

15.4 Legitimate interests can be our own interests of the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.

15.5 Details of our legitimate interest, when used, must be included in our privacy notices.

16 Special Category Data

16.1 Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)

- health
- sexual orientation

16.2 In most cases where we process special categories of personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

16.3 The condition for processing special categories of personal data must comply with the law. If we cannot meet the additional conditions for processing special categories of data that processing activity must cease.

17 Criminal Offence Data

17.1 To process personal data about criminal convictions or offences, EEG must have both a lawful basis and identify a specific conditions for processing in Schedule 1 of the Data Protection Act 2018.

17.2 The Data Protection Act 2018 deals with this type of data in a similar way to special category data (described above), and sets out specific conditions providing lawful authority for processing it.

17.3 EEG will determine its condition for lawful processing of offence data before it begins to process it and this is documented.

18 Individual's Rights

18.1 Individuals have the following rights under UK GDPR:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

19 The Right to be Informed

19.1 Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under UK GDPR.

19.2 EEG must provide individuals with information including; the purpose for processing their personal data, the retention period for that personal data, and who it will be shared with. This is achieved by Privacy Notice's.

19.3 Privacy information must be provided to individuals at the time we collect their personal data from them.

19.4 If we obtain personal data from other sources, we must provide individuals with privacy information within a reasonable period of obtaining the data and this must be no later than within one month.

20 What information must EEG provide?

20.1 What EEG needs to tell people in its privacy information may differ slightly depending on whether we collect the personal data from the individual it relates to or if we obtain it from another source.

20.2 When EEG collects personal data from the individual it relates to, we will provide them with the privacy information at the time we obtain their data.

20.3 When EEG obtains information from a source other than the individual it relates to, EEG will provide the individual with the privacy information:

- Within a reasonable period of obtaining the personal data and no later than one month;
- If the data is used to communicate with the individual, at the latest, when the first communication takes place; or
- If disclosure to someone else is envisaged, at the latest when the data is disclosed.

21 The Right of Access

21.1 Individuals have the right to access their personal data and supplementary information.

21.2 The right of access allows individuals to be aware of and verify the lawfulness of the processing. Under the UK GDPR, individuals have the right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data; and
- Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

21.3 Copies of the information will be provided **free of charge**. However, EEG has the right to charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. A 'reasonable fee' can also be charged to comply with requests for further copies of the same information but this does not mean that EEG will charge for all subsequent access requests.

21.4 Information must be provided without delay and at the latest within one month of receipt of the request for access.

21.5 EEG has the right to extend the period of compliance by a further two months where requests are complex or numerous and if this is the case, the individual will be informed within one month to explain why the extension is necessary.

21.6 Subject Access Requests (SARs) as they are known should be directed to the Group GDPR and Compliance Lead for processing.

22 The Right to Rectification

22.1 UK GDPR gives individuals the right to have personal data rectified. Personal data can be rectified if it is inaccurate or incomplete.

22.2 EEG will respond to a request for rectification within one month. This can be extended by two months where the request for rectification is complex. If the rectification involves multiple recipients EEG must contact each recipient and inform them of the rectification, unless this proves impossible or involves disproportionate effort.

23 The Right to Erasure (the Right to be Forgotten)

23.1 The right to erasure is also known as 'the Right to be Forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

23.2 The right to erasure is not an absolute right. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

a) Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.

b) When the individual withdraws consent.

c) When the individual objects to the processing and there is no overriding legitimate interest for continuing with processing.

d) The personal data was unlawfully processed (i.e. otherwise in breach of the UK GDPR).

e) The personal data has to be erased in order to comply with a legal obligation.

f) The personal data processed in relation to the offer of information society services to a child. Under the UK GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

23.3 EEG can refuse to comply with a request for erasure where the personal data is processed for the following reason(s):

a) To exercise the right of freedom of expression and information;

b) To comply with a legal obligation for the performance of a public interest task or exercise of official authority;

c) For public health purposes in the public interest;

d) Archiving purposes in the public interest, scientific, research, historical research or statistical purposes; or

e) The exercise or defense of legal claims.

23.4 There are extra requirements when the request for erasure relates to children's personal data, reflecting the UKGDPR emphasis on the enhanced protection of such information especially in online environments.

23.5 If an individual asks for their personal information to be erased (or forgotten) you must notify the Group GDPR and Compliance Lead for this request to be processed.

24 The Right to Restrict Processing

24.1 Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, EEG is permitted to store the personal data, but not to process it. EEG is allowed to retain just enough information about the individual to ensure that the restriction is respected in future.

24.2 EEG can restrict the processing of personal data in the following circumstances:

a) Where the individual contests the accuracy of the personal data, EEG will restrict the processing until the accuracy of the personal data is verified.

b) Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interest) and EEG is considering whether there are legitimate grounds that override those of the individual.

c) When processing is unlawful and the individual opposes erasure and requests restriction instead.

d) If EEG no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

24.3 Individuals will be informed when EEG decides to lift a restriction on processing.

25 The Right to Portability

25.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

25.2 The right to data portability only applies to:

- Personal data an individual has provided to EEG;
- Where the processing is based on the individual's consent or for the performance of a contract;
- When processing is carried out by automated means.

25.3 If an individual requests for their personal data to be moved the EEG must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. The information will be provided **free of charge** and EEG will respond without undue delay, and within one month.

25.4 This can be extended by two months where the request is complex or EEG receives a number of requests. The individual will be informed within one month of the receipt of the request if an extension is necessary.

26 The Right to Object

26.1 In some circumstances individuals have the right to object to:

a) processing based on legitimate interest or the performance of a task in the public interest/exercise of official authority (including profiling);

b) direct marketing (including profiling); and

c) processing for purposes of scientific/historical research and statistics.

26.2 EEG will stop processing the personal data unless:

a) it can demonstrate compelling legitimate grounds for processing, which override the interests, rights and freedoms of the individuals; or

b) the processing is for the establishment, exercise or defense or legal claims.

- Individuals will be informed of their right to object "at the point of first communication" and this will be detailed in the privacy notice for that first contact activity.
- EEG will stop processing personal data for direct marketing purposes as soon as it receives an objection. EEG recognises that there are no exemptions or grounds to refuse. EEG will deal with an objection to processing personal data for direct marketing purposes at any time and free of charge. We will inform individuals of their right to object "at the point of first communication" in our privacy notice for that first contact activity.

27 Rights related to automated decision-making including profiling

27.1 The UK GDPR has provisions on:

a) automated individual decision-making (making a decision solely by automated means without any human involvement); and

b) profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

27.2 EEG will only use this type of decision-making where the decision is:

a) necessary for the entry into or performance of a contract; or

b) is authorised by Union or Member state law applicable to EEG; or

c) is based on the individual's explicit consent.

27.3 EEG will make sure that it gives the individual information about the processing and introduces simple ways for them to request human intervention or challenge a decision.

28 Accountability and Governance

28.1 The UK GDPR includes provisions that promote accountability and governance. Ultimately these measures should minimise the risk of breaches and uphold the protection of personal data.

28.2 The Accountability principle requires EEG to demonstrate that it complies with the principles and states explicitly that it is our responsibility.

28.3 Compliance will be demonstrated by:

a) implementing appropriate technical and organisational measures that ensure and demonstrate that we comply. This includes internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies;

b) maintaining relevant documentation on processing activities;

c) appointing a Data Protection Officer;

d) implementing measures that meet the principles of data protection by design and data protection by default. Measures include:

- Data minimisation;
- Pseudonymisation;
- Transparency;
- Allowing individuals to monitor processing; and
- Creating and improving security features on an ongoing basis
- Using data protection impact assessment where appropriate.

29 Contracts

29.1 As a data controller, we must have written contracts in place with any third party data controllers (and/or) data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

29.2 As a data controller, we must only appoint processors who can provide sufficient guarantees under UK GDPR and that the rights of data subjects will be respected and protected.

29.3 Our contracts must comply with the UK GDPR contractual clauses and where applicable, the requirements set out by the ICO. Our contracts must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

29.4 At a minimum, our contracts must include terms that specify:

a) Acting only on written instructions

b) Those involved in processing the data are subject to a duty of confidence

c) Appropriate measures will be taken to ensure the security of the processing

d) Sub-processors will only be engaged with the prior consent of the controller and under a written contract

e) The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under UK GDPR

f) The processor will assist the controller in meeting its UK GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments (DPIA)

g) Delete or return all personal data at the end of the contract

h) Submit to regular audits and inspections and provide whatever information necessary for the controller and processor to meet their legal obligations.

i) Nothing will be done by either the controller or processor to infringe on UK GDPR.

30 Documentation

30.1 The UK GDPR contains explicit provisions about documenting processing activities. EEG will maintain records such as processing purposes, data sharing and retention. They are kept up to date and reflect our current processing activities.

31 Data Protection Impact Assessments

31.1 A Data Protection Impact Assessment (DPIA) is a process that EEG uses to identify and minimise the data protection risks of an activity (project).

31.2 A DPIA is used for specific listed types of processing, or any other processing that is likely to result in high risk to an individual.

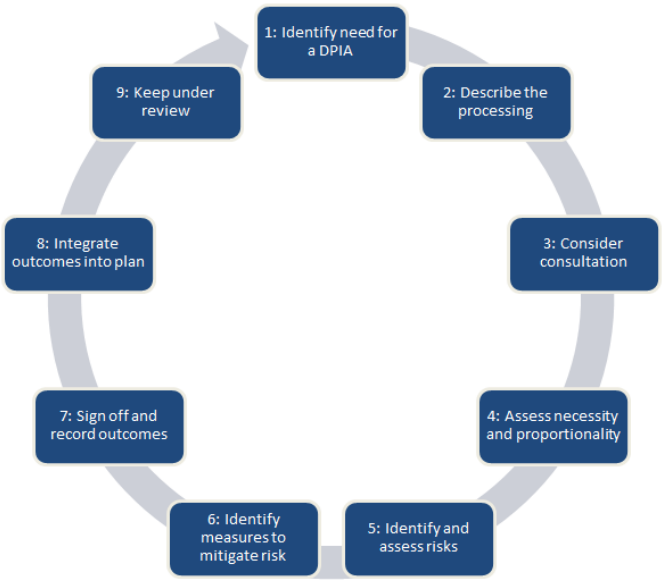
31.3 The DPIA:

- Describes the nature, scope, context and purposes of the processing;
- Assesses necessity, proportionality and compliance measures;
- Identifies and assesses risks to individuals; and
- Identifies any additional measures to mitigate those risks.

31.4 To assess the level of risk EEG considers both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

31.5 You must consult with EEG Group GDPR and Compliance Lead, who will assist you in carrying out the DPIA with the support of the Data Protection Officer (DPO). If a high risk is identified and the risk cannot be mitigated, EGG will consult with the ICO (Information Commissioners Officer) before starting the processing. The ICO will give written advice within eight weeks, or fourteen weeks in complex cases and where appropriate they may issue a formal warning not to process the data or ban the processing altogether.

31.6 A DPIA should begin early in the life of an activity (project), before EEG starts processing, it will plan and develop the activity using this nine step process:



32 Data Protection Officer

32.1 The UK GDPR places a duty upon EEG to appoint a Data Protection Officer (DPO).

32.2 The DPO helps EEG to monitor internal compliance, informs and advises on our data protection obligations, provides advice about DPIAs and acts as the contact point with the ICO.

32.3 The DPO is an independent expert in Data Protection who has been externally appointed by EEG.

32.4 Contact with EEG's DPO can be made through the Group GDPR and Compliance Lead. The responsibilities of the DPO are:

a) To inform and advise EEG's and its employees about our obligations to comply with the

b) UK GDPR and other data protection laws;

c) To monitor compliance with the UK GDPR and other data protection laws, and with our data protection policies, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;

d) To advise on, and to monitor data protection impact assessments (DPIAs)

e) To cooperate with the ICO; and

f) Be the first point of contact for the ICO.

33 Security

33.1 The UK GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

33.2 You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

34 Storing data securely

a) In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it

b) Printed data should be shredded when it is no longer needed

c) Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.

d) Data stored external storage must be encrypted or password protected and locked away securely when they are not being used

e) The DPO must approve any cloud used to store data

f) Servers containing personal data must be kept in a secure location, away from general office space

g) Data should be regularly backed up in line with the company's backup procedures

h) Data should never be saved directly to mobile devices such as laptops, tablets or smartphones

i) All servers containing sensitive data must be approved and protected by security software

j) All possible technical measures must be put in place to keep data secure

35 Data retention

35.1 We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

36 International Transfers

36.1 The UK GDPR imposes restrictions on the transfer of personal data outside the UK, to third countries or international organisations.

36.2 These restrictions are in place to ensure that the level of protection of individuals afforded by the UK GDPR is not undermined.

37 Personal Data Breaches

37.1 The UK GDPR places a duty upon EEG to report certain types of personal data breaches to the ICO within 72 hours of becoming aware of the breach, where feasible.

37.2 It is of paramount importance that you report any breach to the Group GDPR and Compliance Lead immediately.

37.3 If the breach is likely to result in high risk of adversely affecting individuals' rights and freedoms, EEG will seek the advice of the DPO before informing those individuals without undue delay.

37.4 EEG has a robust breach investigation and internal reporting procedure in place with the support of the DPO.

37.5 A record of any personal data breach, regardless of whether EEG is required to notify the DPO is held in the Data Breach register, maintained by the Group GDPR and Compliance Lead.

37.6 A Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

37.7 A Personal Data Breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability or personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data and passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

37.8 When reporting a breach to the Group GDPR and Compliance Lead you must provide:

a) A description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned; and
- The categories and approximate number of personal data records concerned;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

37.9 Notification to the ICO of a data protection breach is made by no-one other than EEG appointed DPO.

37.10 Failing to notify a breach when required to do so can result in a significant regulatory fine, so it is important that as soon as you are aware that a breach has occurred, you notify the Group GDPR and Compliance Lead immediately.

38 Children

38.1 Children need particular protection when we collect and process their personal data because they may be less aware of the risks involved.

38.2 Where EEG relies on consent as our lawful basis for processing their personal data, only children aged 13 or over are considered able to provide their own consent. This is the age proposed in the Data Protection Act 2018.

38.3 For children under the age of 13 EEG will obtain consent from whoever holds parental responsibility for the child.

39 Failure to comply

39.1 We take compliance with this policy very seriously. Failure to comply puts both you and EEG at risk.

39.2 The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal.

39.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact the Group GDPR and Compliance Lead.

STUDENT WELFARE, COUNSELLING AND CHILD PROTECTION RECORDS	
PURPOSE	To give a clear guide to those attached to the Counselling and Student Welfare Department, on the writing and keeping of learner notes, of a sensitive nature
SCOPE	All learner Counselling, Welfare, Chaplaincy and Child Protection Officer Records
RESPONSIBILITY	All Student Welfare Staff and volunteer staff

1. Procedures for Child Protection Records

1.1. No notes are to be removed from the College premises without the written consent of the Group Head of Welfare and Safeguarding.

1.2. All notes must be written on college premises on the day the individual is seen. These records are kept on Intuition, the database held by Student Welfare.

1.3. All handwritten notes are to be written in ink, each entry dated, timed and signed. These will be updated when needed. They will be scanned and stored on SharePoint.

1.4. Records are kept in accordance with NSPCC Child Protection guidelines to a child's 25th birthday e.g. 9 years after school files are received.

1.5. Access can be given to other trained Child Protection Officers within the College. These are currently Group Principal Colin Shaw, Seniors DSL Andrew Adamson and Stuart Small, Student Welfare Manager (WSC), Senior Welfare Officers and Welfare Officers in the group.

1.6. These records may need to be given on request to Social Services, the Police or a Court if a Child Protection Conference is called. The Child Protection Co-ordinator will need to be notified if this happens.

2. Procedure for Welfare records

2.1. All notes must be recorded on to the Welfare database currently called 'Intuition' in real time with the client present.

2.2. No information can be removed from the college premises without the noted consent of the Group Head of Welfare and Safeguarding.

2.3. Access to the database is limited to the Student Welfare Staff who are authorised users. Any handwritten information must be scanned and kept securely on SharePoint.

2.4. Welfare records should only be kept for 9 years (up to a Childs 25th Birthday).

3. Procedure for Counselling and Chaplaincy Records. Chaplaincy is included in the word counselling / counsellor.

3.1. Dates and times of meetings will be added to 'Intuition'.

3.2. All notes must be written on college premises on the day the individual is seen.

3.3. All handwritten notes are to be written in ink, each entry dated, timed and signed and placed in the students file.

3.4. All records will be kept in a locked cabinet and the counsellor will hold the key.

3.5. Records will be kept for three years from the last entry and are then securely disposed.

3.6. Counselling records can only be handed over to a court of law or to the police.

3.7. The Counselling Service ensures confidentiality of client's personal data, subject to the following exceptions:-

a) Where the Counsellor has the express consent of the client to disclose the data.

b) Where the Counsellor reasonably believes that the client is a serious danger to themselves, that their GP should be informed of that fact so that appropriate steps can be taken to ensure their safety, and that to inform the client of the disclosure would increase the level of risk;

c) Where the Counsellor reasonably believes that serious harm may befall a third party if the data were not disclosed;

d) Where the Counsellor would be liable to civil or criminal court procedure if the data were not disclosed.

4. NSPCC

4.1. The guidance for education on record keeping and management of child protection information states that:

Child protection files should be passed on to any new school the child attends and kept until they are 25 (this is 9 years after they reach the school leaving age) (IRMS, 2016).

British association of counsellors and psychotherapists

5. How long should I keep my records for?

5.1. UK GDPR does not set specific time limits but requires that you only keep information for as long as is necessary for the specific reason that you originally collected it.

5.2. Where possible we will anonymise our records – this is the same as deletion, as UK GDPR does not apply to anonymous data. The information however must be truly anonymous so that there is no way that the data subject can be identified.

5.3. We will consider whether we can minimise a record after a certain time. So that some of the information we hold can be deleted (especially the more sensitive information) so as to just retain the limited data.

5.4. When deciding how long we will keep information for we will consider:

a) whether the data in our records is covered by any legal or regulatory requirements

b) whether our indemnity insurers specify a time period

c) our organisational policies

d) the time limits for raising a complaint against a therapist (currently three years after counselling has ended under our Professional Conduct procedure)

e) https://www.bacp.co.uk/about-us/contact-us/gdpr

Revision History

Date	Reason	Section Number	Changes Made
Dec 2023	Harmonisation	All	Conversion of SAT & WSC policies to create EEG version.
			Re-numbering throughout.
			Removal of Appendix 2 – Divulging information to absent parents.
			Changes to wording throughout, removal of DPL – changed to Group GDPR and Compliance Lead.
			Updated wording changes in line with Brexit.
		2.12	Addition of 4policies link for staff to access all updated and current policies.