GRACE FOUNDATION - DATA PROTECTION POLICY

1. Introduction

This Data Protection Policy applies to Grace Foundation, (The Gate, International Drive, Shirley, Solihull, B90 4WA) Charity no. 1103021 Company no. 5003276. Grace Foundation is a charitable subsidiary of IM Group Ltd. This Policy sets Grace Foundation's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by Grace Foundation, its employees, agents, contractors, or other parties working on behalf of Grace Foundation.

2. Definitions

"consent"	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them;
"data controller"	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, Grace Foundation is the data controller of all personal data relating to the data subjects used in our business for our commercial purposes;
"data processor"	means a natural or legal person or organisation which processes personal data on behalf of a data controller;
"data subject"	means a living, identified, or identifiable natural person about whom Grace Foundation holds personal data;
"EEA"	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway;
"personal data"	means any information relating to an identified or identifiable natural person ('data subject'); who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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 data subject;
"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 transmitted, stored, or otherwise processed
"processing	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"pseudonymisation"	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is

subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person

3. **Scope**

Grace Foundation is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

Grace Foundation's Data Protection Officer can be contacted at dpo@imgroup.co.uk. The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

The policy relates to all staff (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with Grace Foundation in the UK or overseas) within the organisation and has been created to ensure that staff deal with the area that this policy relates to in accordance with legal, regulatory, contractual and business expectations and requirements.

All Directors and Line Managers are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of Grace Foundation comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

Any questions relating to this Policy or to Data Protection Law should be referred the Data Protection Officer. In particular, the Data Protection Officer should always be consulted in the following cases:

a) if there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed;
b) if consent is being relied upon in order to collect, hold, and/or process personal data;
c) if there is any uncertainty relating to the retention period for any particular type(s) of personal data;
d) if any new or amended privacy notices or similar privacy-related documentation are required;
e) if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of subject access requests);
f) if a personal data breach (suspected or actual) has occurred;
g) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data;
h) if personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors);
i) if personal data is to be transferred outside of the UK and there are questions relating to the legal basis on which to do so;
j) when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment;
k) when personal data is to be used for purposes different to those for which it was originally collected;

4.

The Data Protection Principles

This Policy aims to ensure compliance with Data Protection Law. The UK GDPR sets out the following principles with which any party handling personal data must comply. Data controllers are responsible for, and must be able to demonstrate, such compliance. All personal data must be:

4.1 processed lawfully, fairly, and in a transparent manner in relation to the data subject;

4.2 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;

4.3 adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;

4.4 accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;

4.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 UK GDPR in order to safeguard the rights and freedoms of the data subject;

4.6 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.

5. **The Rights of Data Subjects**

The UK GDPR sets out the following key rights applicable to data subjects:

5.1 The right to be informed;

5.2 The right of access;

5.3 The right to rectification;

5.4 The right to erasure (also known as the 'right to be forgotten');

5.5 The right to restrict processing;

5.6 The right to data portability;

5.7 The right to object; and

5.8 Rights with respect to automated decision-making and profiling.

6. **Lawful, Fair, and Transparent Data Processing**

6.1 Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the processing of personal data shall be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;

c) the processing is necessary for compliance with a legal obligation to which the data controller is subject;

d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

6.2 If the personal data in question is special category personal data (also known as "sensitive personal data"), at least one of the following conditions must be met:

a) the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the law prohibits them from doing so);

b) the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by law or a collective agreement pursuant to law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

c) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

e) the processing relates to personal data which is manifestly made public by the data subject;

f) the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

g) the processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

h) the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR;

i) the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

j) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19 of the Data Protection Act 2018) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

7. Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

7.1 Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.

7.2 Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.

7.3 Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.

7.4 If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.

7.5 For special category personal data processed, we Grace Foundation shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question is issued with a suitable privacy notice in order to capture their consent.

7.6 In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records are kept of all consents obtained in order to ensure that Grace Foundation can demonstrate its compliance with consent requirements.

8. Specified, Explicit, and Legitimate Purposes

8.1 Grace Foundation collects and processes the personal data collected directly from data subjects and personal data obtained from third parties.

8.2 Grace Foundation only collects, processes, and holds personal data for specific purposes.

8.3 Data subjects are kept informed at all times of the purpose or purposes for which Grace Foundation uses their personal data, through the individual Educational Trusts. Please refer to Part 15 for more information.

9. Adequate, Relevant, and Limited Data Processing

9.1 Grace Foundation will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed.

9.2 Employees, agents, contractors, or other parties working on behalf of Grace Foundation may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data will not be collected.

9.3 Employees, agents, contractors, or other parties working on behalf of Grace Foundation may process personal data only when the performance of their job duties requires it. Personal data held by Grace Foundation cannot be processed for any unrelated reasons.

10. Accuracy of Data and Keeping Data Up-to-Date

10.1 Grace Foundation shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 17, below.

10.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

11. Data Retention

11.1 Grace Foundation shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

11.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

11.3 For full details of Grace Foundation's approach to data retention, including retention periods for specific personal data types held by Grace Foundation, please refer to IM Groups Data Retention Policy.

12. Secure Processing

12.1 Grace Foundation shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 24 to 29 of this Policy.

12.2 All technical and organisational measures taken to protect personal data are regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.

12.3 Data security is maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:

a) only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;

b) personal data is kept accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and

c) authorised users are only able to access the personal data as required for the authorised purpose or purposes.

13. Accountability and Record-Keeping

13.1 The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

13.2 Grace Foundation shall follow a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects.

13.3 All employees, agents, contractors, or other parties working on behalf of Grace Foundation shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Company policies.

13.4 Grace Foundation's data protection compliance shall be regularly reviewed and evaluated on an ongoing basis.

13.5 Grace Foundation keeps written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) the name and details of Grace Foundation, its Data Protection Officer, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);

b) the purposes for which Grace Foundation collects, holds, and processes personal data;

c) Grace Foundation's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data;

d) details of the categories of personal data collected, held, and processed by Grace Foundation, and the categories of data subject to which that personal data relates;

e) details of any transfers of personal data to non-UK countries including all mechanisms and security safeguards;

f) details of how long personal data will be retained by Grace Foundation (please refer to IM Groups Data Retention Policy);

g) details of personal data storage, including location(s);

h) detailed descriptions of all technical and organisational measures taken by Grace Foundation to ensure the security of personal data.

14. Data Protection Impact Assessments and Privacy by Design

14.1 In accordance with the privacy by design principles, Grace Foundation carries out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.

14.2 The principles of privacy by design are followed at all times when collecting, holding, and processing personal data. The following factors should be taken into consideration:

a) the nature, scope, context, and purpose or purposes of the collection, holding, and processing;
b) the state of the art of all relevant technical and organisational measures to be taken;
c) the cost of implementing such measures; and
d) the risks posed to data subjects and to Grace Foundation, including their likelihood and severity.

14.3 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

a) the type(s) of personal data that will be collected, held, and processed;
b) the purpose(s) for which personal data is to be used;
c) Grace Foundation's objectives;
d) how personal data is to be used;
e) the parties (internal and/or external) who are to be consulted;
f) the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
g) risks posed to data subjects;
h) risks posed both within and to Grace Foundation; and
i) proposed measures to minimise and handle identified risks.

15. Keeping Data Subjects Informed

15.1 Grace Foundation, through the Educational Trusts that Grace Foundation are contracted to work with, shall provide the information set out in Part 15.2 to every data subject:

a) where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
b) where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
    i) if the personal data is used to communicate with the data subject, when the first communication is made; or
    ii) if the personal data is to be transferred to another party, before that transfer is made; or
    iii) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

15.2 The following information shall be provided in the form of a privacy notice:

a) details of Grace Foundation the name and contact details of its Data Protection Officer;
b) the purpose(s) for which the personal data is being collected and will be processed and the lawful basis justifying that collection and processing;
c) where applicable, the legitimate interests upon which Grace Foundation is justifying its collection and processing of the personal data;
d) where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
e) where the personal data is to be transferred to one or more third parties, details of those parties;
f) where the personal data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place;
g) details of applicable data retention periods;
h) details of the data subject's rights under the UK GDPR;
i) details of the data subject's right to withdraw their consent to Grace Foundation's processing of their personal data at any time;

j) details of the data subject's right to complain to the Information Commissioner's Office;

k) where the personal data is not obtained directly from the data subject, details about the source of that personal data;

l) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

m) details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

16. Data Subject Access

16.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which Grace Foundation holds about them, what it is doing with that personal data, and why.

16.2 Responses to SARs will normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

16.3 All SARs received shall be handled by Grace Foundation's Data Protection Officer.

16.4 Grace Foundation does not charge a fee for the handling of normal SARs. Grace Foundation reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

17. Rectification of Personal Data

17.1 Data subjects have the right to require Grace Foundation to rectify any of their personal data that is inaccurate or incomplete.

17.2 Grace Foundation shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing Grace Foundation of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

17.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

18. Erasure of Personal Data

18.1 Data subjects have the right to request that Grace Foundation erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for Grace Foundation to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

b) the data subject wishes to withdraw their consent to Grace Foundation holding and processing their personal data;

c) the data subject objects to Grace Foundation holding and processing their personal data (and there is no overriding legitimate interest to allow Grace Foundation to continue doing so) (see Part 21 of this Policy for further details concerning the right to object);

d) the personal data has been processed unlawfully;

e) the personal data needs to be erased in order for Grace Foundation to comply with a particular legal obligation.

18.2 Unless Grace Foundation has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months

in the case of complex requests. If such additional time is required, the data subject shall be informed.

18.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

19. Restriction of Personal Data Processing

19.1 Data subjects may request that Grace Foundation ceases processing the personal data it holds about them. If a data subject makes such a request, Grace Foundation shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

19.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

20. Objections to Personal Data Processing

20.1 Data subjects have the right to object to Grace Foundation processing their personal data based on legitimate interests, for direct marketing (including profiling).

20.2 Where a data subject objects to Grace Foundation processing their personal data based on its legitimate interests, Grace Foundation shall cease such processing immediately, unless it can be demonstrated that Grace Foundation's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

20.3 Where a data subject objects to Grace Foundation processing their personal data for direct marketing purposes, Grace Foundation shall cease such processing promptly.

21. Personal Data Collected, Held, and Processed

To enable Grace Foundation to fully prepare for and comply with the data protection laws, we have carried out a data protection information audit to better enable us to record, categorise and protect the personal data that we hold and process. The audit has identified, categorised and recorded all personal information obtained, processed and shared by our group in our capacity as a controller and has been compiled on a central register which includes: -

23.1 What personal data we hold
23.2 Where it came from
23.3 Who we share it with
23.4 Legal basis for processing it
23.5 What format(s) is it in
23.6 Who is responsible for it?
23.7 Access level (i.e., full, partial, restricted etc)
23.8 We have also carried out an information audit in our capacity as a data processor, having identified, categorised, and recorded all personal information that we process on behalf of a controller (or joint controllers).
See Appendix A for details.

22. Data Security - Transferring Personal Data and Communications

Grace Foundation shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

24.1 All emails containing personal data is password protected/encrypted;
24.2 All emails containing personal data shall be marked "confidential";
24.3 Where personal data is to be transferred in hardcopy form it will be passed directly to the recipient or sent using a signed for delivery service;

24.4 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential" and if in electronic format password protected;

Data Security - Storage
Grace Foundation shall ensure that the following measures are taken with respect to the storage of personal data:

25.1 All electronic copies of personal data are stored securely using passwords;
25.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media are stored securely in a locked box, drawer, cabinet, or similar;
25.3 All personal data stored electronically are backed up daily with backups stored onsite (where?). All backups are encrypted.
25.4 No personal data is transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of Grace Foundation and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Grace Foundation where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the applicable Data Protection Law (which may include demonstrating to Grace Foundation that all suitable technical and organisational measures have been taken);

23. Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it is securely deleted and disposed of. All personal data is disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion) and priorities the protection of the personal data at all times. For further information on the deletion and disposal of personal data, please refer to IM Group's Data Retention Policy.

24. Data Security - Use of Personal Data

Grace Foundation ensures through training and awareness that the following measures are taken with respect to the use of personal data:

27.1 No personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of Grace Foundation requires access to any personal data that they do not already have access to, such access should be formally requested from the IM Group IT Team, with prior approval by the owner of the data or the individual's Line Manager;

27.2 No personal data may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of Grace Foundation or not, without the authorisation of the Data Protection Officer;

27.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, contractors, or other parties at any time;

27.4 If personal data is being viewed on a computer screen and the computer in question is left unattended for any period of time, the user locks the computer and screen before leaving it;

25. Data Security - IT Security

Grace Foundation shall ensure that the following measures are taken with respect to IT and information security:

28.1 All passwords used to protect personal data are changed regularly and do not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols;

28.2 Under no circumstances are any passwords written down or shared between any employees, agents, contractors, or other parties working on behalf of Grace Foundation, irrespective of seniority or department. If a password is forgotten, it is reset using the applicable method. IT staff do not have access to passwords;

28.3 All software (including, but not limited to, applications and operating systems) are kept up-to-date. IT staff (IM Group) are responsible for installing any and all security-related updates when the updates are made;

28.4 No software is installed on any Company-owned computer or device without the prior approval of the IT team at IM Group.

26. Organisational Measures

Grace Foundation shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

29.1 All employees, agents, contractors, or other parties working on behalf of Grace Foundation shall be made fully aware of both their individual responsibilities and Grace Foundation's responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy;

29.2 Only employees, agents, contractors, or other parties working on behalf of Grace Foundation that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by Grace Foundation;

29.3 All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data;

29.4 All employees, agents, contractors, or other parties working on behalf of Grace Foundation handling personal data will be appropriately trained to do so;

29.5 All employees, agents, contractors, or other parties working on behalf of Grace Foundation handling personal data will be appropriately supervised;

29.6 All employees, agents, contractors, or other parties working on behalf of Grace Foundation handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

29.7 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

29.8 All personal data held by Grace Foundation shall be reviewed periodically, as set out in IM Group's Data Retention Policy;

29.9 The performance of those employees, agents, contractors, or other parties working on behalf of Grace Foundation handling personal data shall be regularly evaluated and reviewed;

29.10 All employees, agents, contractors, or other parties working on behalf of Grace Foundation handling personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract;

29.11 All agents, contractors, or other parties working on behalf of Grace Foundation handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of Grace Foundation arising out of this Policy and Data Protection Law;

29.12 Where any agent, contractor or other party working on behalf of Grace Foundation handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless Grace Foundation against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure;

27. Transferring Personal Data to a Country Outside the UK

Grace Foundation will not transfer (in the form of making available remotely) personal data to countries outside of the UK (EEA).

28. Data Breach Notification

31.1 All personal data breaches are reported immediately to Grace Foundation's Data Protection Officer.

31.2 If an employee, agent, contractor, or other party working on behalf of Grace Foundation becomes aware of or suspects that a personal data breach has occurred, they will not attempt to investigate it themselves.

31.3 The Data Protection Officer will complete a 'Self-assessment for data breaches form'. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g., financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer will ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

31.4 A 'Data Incident Report Form' is completed by the Data Protection Officer' for all reportable and non-reportable data breaches and filed on a secure SharePoint. This will include Data lost, Security of data, How many individuals have been affected, Explanation of facts leading to loss, who lost the data, when it was lost, who received the data, Give an explanation of any steps taken so far to retrieve the data, Record of action taken, Has the data been recovered/destroyed, Who else has been notified, whether the individual who caused the data breach has had any training and if so, when the training was received.

31.5 In the event that a personal data breach occurs, the IM Group IT team will ensure that all affected data subjects are informed of the breach directly and without undue delay.

31.6 Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal data records concerned;

c) The name and contact details of Grace Foundation's data protection officer (or other contact point where more information can be obtained);

d) The likely consequences of the breach;

e) Details of the measures taken, or proposed to be taken, by Grace Foundation to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

29. Implementation of Policy

This Policy shall be deemed effective as of 10/02/2023. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

APPENDIX A

Grace Foundation Information Audit – November 2022

- **Key =** PS refers to Partner School
- **SIMS (or equivalent) =** refers to any management information system used by Schools of which they remain the Data Controller and grant GF access to data share
- **CPOMS (or equivalent) =** refers to any safeguarding information system used by Schools of which they remain the Data Controller and grant GF access to data share

Whose personal data do we collect ie: students, parents, volunteers, staff, governors, contractors, 3rd party providers	**PURPOSE**	**What personal data do we collect/use?**	**What personal data do we hold?**	**Where did the data come from?**	**What do we use it for?**	**Who do we share it with?**	**Do we need to keep this information? If so give reason why.**	**Where is the information stored?**	**If we do not keep the information, how is it deleted or destroyed?**	**How long do we need to keep this information?**	**Is consent required to use this information?**	**Does the information need to be archived?**	**Action (s) and date to be completed by**
PARENTS/CARERS	**Parental engagement**	Data (information) given by parents verbally – with the duty to record correctly and pass on promptly to PS. This could include personal information, parents wishing to withdraw students from RSE/ R.E/ Ethos events or information relating to personal concerns and family issues.	Information is passed onto PS and held on their SIMS (or equivalent), or Safeguarding Systems (i.e.: CPOMs or equivalent.) Digital Records of interventions and concerns will be kept by Ethos Team with non-identifiers used for Student or Parent Names. These will be password protected if containing sensitive data.	Sims, Safeguarding system or equivalent. Direct from data subject.	Supporting parents. Updating agencies. Updating records. Ensuring students are safe.	Internal PS use. Reporting to GF (no personal identifiers used). Internal/ External agencies for safeguarding purposes.	Yes. Student information so needed during their time at school and up till they are 25yrs.	CPOMS. SIMS. Secure Ethos Team Staff records.	Securely deleted on electronic servers or hard copies destroyed confidentially.	Kept during time student is at school and up till they are 25yrs.	Special category data shared by PS to GF.	No	GPDR Update and Training for all Staff in January 2023.
STUDENTS	**Students taking part in events /lessons/ experiences organised by the Ethos Team.**	Name, form, year, any issues, safeguarding information, what content they took part in.	Name, form, year, what content they took part in – in order to organise and deliver effective educational activities.	SIMS, CPOMS or equivalent.	To document who took part in specific events, clubs, and activities for educational purposes.	Internal PS use. Reporting to GF (no personal identifiers used). Internal/ External agencies for safeguarding purposes.	Yes, in order to document students' involvement in activities.	CPOMS. SIMS. Secure Ethos Team Staff records.	Securely deleted on electronic servers or hard copies destroyed confidentially.	For annual impact reporting records.	Yes. Parental consent given to PS who are able to share with GF under usage for legitimate purposes.	No	GPDR Update and Training for all Staff in January 2023.
STUDENTS	**Photo/ Video footage from Ethos Team led events and activities.**	Images of students - used only if parental consent release is given to PS for promotional use.	Images (not named) – May include date, venue, and nature of event.	Photos and videos taken during events with no personal student identifiers.	To document events for measuring impact and reporting.	School. Impact Reports. Promotional (if consented).	Yes – anonymised for programme records.	Online/ Notice boards/ Ethos files/social media	Deleted if no longer required.	For annual impact reporting records and online social media use.	Yes. Parental consent given to PS.	No	GPDR Update and Training for all Staff in January 2023.

WHOSE DATA?	PURPOSE	What personal data do we collect/use?	What personal data do we hold?	Where did the data come from?	What do we use it for?	Who do we share it with?	Do we need to keep this information? If so give reason why.	Where is the information stored?	If we do not keep the information, how is it deleted or destroyed?	How long do we need to keep this information?	Is consent required to use this information?	Does the information need to be archived?	Action (s) and date to be completed by
STUDENT	**Intranet – Impact Reporting System**	Impact reports containing depersonalised impact data from all Ethos Activities including mentoring,	Anonymised feedback information from students. - Year Group. Gender. Opinions and views on content delivery.	Work of the Ethos Team	Reporting to Schools, OFSTED, Key Stakeholders	School use, OFSTED inspectors, Stakeholders	Yes - in order to report on effectiveness of the team and for safeguarding/pastoral purposes	Online, Secured Server	NA	3 Years to be able to report on impact over time	Special category data shared by PS to GF.	No	Annual Review – Sept 23
STUDENTS	**Feedback forms from events / lessons/ interventions**	Anonymised feedback information from students. - Opinions and views on content delivery. Or specific named feedback for safeguarding interventions.	Anonymised feedback information from students. - Year Group. Gender. Opinions and views on content delivery.	Survey forms	To ensure that we provide good quality education. For feedback and impact reporting.	Internal PS use. Internal/ External agencies for safeguarding purposes.	Yes. To demonstrate impact of activity	Ethos Team Staff records.	Feedback forms disposed of after academic year. Feedback summaries kept on file. Online is not timebound.	No requirement due to no personal information stored long term.	No	No	Annual Review – Sept 23
STUDENTS	**Ethos Trips and Visits led by the Cross Academy Support Team.**	Students Passport details (if overseas trip), name, gender, age, individual medical information inc. doctors' details, parents/Carers names, personal contact details (phone/address/email)	Students Passport details, EHIC details, name, gender, age, individual medical information inc. doctors' details, parents/Carers names, personal contact details (phone/address/email)	Passport, Medical & student form/consent SIM's	Trip paperwork, Risk Assessment, in accordance with insurance needs.	Accompanying staff & Leaders Emergency Key Staff listed on Trip paperwork, Trip provider	Consent forms are put into confidential waste after the event. Digital copies and Trip paperwork is kept for the current year plus one.	CPOMS. SIMS. Ethos Team Staff records.	Physical Consent forms - these are put into the confidential waste after use.	Digital records kept for Academic Year plus one.	Yes – at source from forms	No	GPDR Update and Training for all Staff in January 2023.
STUDENTS	**Intervention Groups / Mentoring**	Pupils names, targets, SEN Status, PP Status, Prior attainment, All Data including safeguarding and behaviour issues/concerns	Pupils names, targets, SEN Status, PP Status, Prior attainment, All Data including safeguarding and behaviour issues/concerns	SIMS, CPOMS, School staff	Analysis of student information and progress. Intervention planning for pupils	Pastoral and academic staff where necessary to track pupil progress. Shared with Ethos Team.	Yes, whilst groups are with functioning.	Online. SIMS. Secure Staff records.	Securely deleted on electronic servers or hard copies destroyed confidentially.	Kept during time student is at school and up till they are 25yrs.	Special category data shared by PS to GF.	No	GPDR Update and Training for all Staff in January 2023.

STUDENTS	**Phone calls/ Emails giving data (information) about pupils**	Relevant information such as pupils names, targets reasons for the email ie behaviour.	Pupils' names/targets/information relevant to the teaching/support of the pupils,	SIMS. Personal experience of students/families	Planning and supporting pupils in developing and progressing.	Relevant people included in email depending on issue, either teaching staff or support staff for behaviour.	Dependent on information, it may be added to class data file or deleted once read.	Secure Staff records.	Physical copies shredded after use. If on email it will be deleted from server.	Kept during time student is at school and up till they are 25yrs.	Special category data shared by PS to GF or given directly by parent/child.	No	GPDR Update and Training for all Staff in January 2023.
WHOSE DATA?	**PURPOSE**	**What personal data do we collect/use?**	**What personal data do we hold?**	**Where did the data come from?**	**What do we use it for?**	**Who do we share it with?**	**Do we need to keep this information? If so give reason why.**	**Where is the information stored?**	**If we do not keep the information, how is it deleted or destroyed?**	**How long do we need to keep this information?**	**Is consent required to use this information?**	**Does the information need to be archived?**	**Action (s) and date to be completed by**
STAFF	**Personal Information for new and existing staff**	Name, Address, Personal details, Work history, Ethnicity etc	Name, Address, Personal details, Work history, Ethnicity etc	Application form / Cascade	Holding staff information and details on Cascade	Internal use and shared with PS for their SINGLE CENTRAL RECORD in line with SLA	Yes - ongoing staff	Cascade	Deleted after staff leave in line with IMG policy	As long as staff member present	Individuals pass on the information to us.	No	Annual Review – Sept 23
STAFF	**To obtain DBS Certificate (processed by GF not IMG)**	ID Documents, Personal info	ID Documents, Personal info, Criminal record info	Data subject	Processing DBS certificate and Safeguarding	Internal use and shared with Partner Schools for their SINGLE CENTRAL RECORD in line with SLA	Yes- Safeguarding reasons	Secure online.	Deleted after staff leave in line with IMG policy	As long as staff member present	Yes - given at source	No	GPDR Update and Training for all Staff in January 2023.
STAFF	**Employee Expenses**	Bank details	Bank details	Data subject	Processing employee expenses	Internal use	Yes - ongoing	Online - BANKLINE and QuickBooks	Deleted	As long as staff member present	Yes - given at source	No	Annual Review – Sept 23
STAFF	**Entry to GATE**	Car Registration	Car Reg	Data subject	Entry to Gate	IM GROUP HQ	Yes - ongoing entry to Gate	Cascade	Deleted	As long as staff member present	Yes - given at source	No	Annual Review – Sept 23
POTENTIAL STAFF	**Job Application forms or Online Applications**	Name, Address, Personal details, Work history, Ethnicity etc	Name, Address, Personal details, Work history, Ethnicity etc	Application form or online application via job site.	Processing Job Applications	Internal use - and PS for job interviews	Yes - for job applications	Secure online files. Secure locked cupboard.	Shredded if doesn't need to be stored.	Yes - kept up to 3 months after for recruitment.	Yes - given at source	No	Ensure Application forms up to date with latest policy compliance.
GENERAL PUBLIC	**Website: Enquiring about our organisation and its work. Subscribing to email updates. Site Activity**	Name, email, message, Web cookies	Name, email, message, Web cookies	Online Collection	Processing enquiries. Maintaining efficient web	Internal use	Yes - for communication reasons	Online	Deleted	Up to 1 year	Yes - given at source	No	Annual Review – Sept 23

EXTERNAL GROUPS	**Regular providers such as church partners, Message Trust, YFC, Loudmouth, Riverside etc**	Proof of DBS/ who they work for/ training details, Name, Address, Contact info	Proof of DBS/ who they work for/ training details, Name, Address, Contact info	Data subject	To check suitability to work unaccompanied in school	Internal School use- only or checked by Ofsted inspectors / Serious issues if required	Yes- Safeguarding reasons, also for contacting groups	Online. SIMS. Secure Staff records. Intranet	Shredded if doesn't need to be stored.	As long as they are a provider	Yes - given at source	No	Annual Review – Sept 23
VOLUNTEERS	**People volunteering to work with Ethos Team**	Proof of DBS/ Personal information and details	Proof of DBS/ Personal information and details	Data subject	To check suitability to work unaccompanied in school	Internal School use- only or checked by Ofsted inspectors / Serious issues if required	Yes- Safeguarding reasons	Online. SIMS. Secure Staff records.	Shredded if doesn't need to be stored.	As long as volunteer present	Yes - given at source	No	Annual Review – Sept 23