THE GREIG TRUST

Incorporating

THE HS & SV AND D & M GREIG FUNDS
THE DAVID GREIG EDUCATIONAL TRUST

DATA SECURITY POLICY

1. Purpose of this policy

1.1 The Greig Trust (the **"Trust"**) takes the security of the personal data which it holds very seriously, and all Trustees and the Trust Administrator must understand the importance of ensuring that personal data is secure.

1.2 The Data Protection Act 1998 (the **"Act"**) requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. This means not only ensuring that the personal data is not stolen or accessed by inappropriate people, but also ensuring that the data is not accidentally lost, damaged or destroyed.

1.3 "**Personal data**" in this context means any information from which a living individual can be identified (either from that information alone, or in conjunction with other information which we hold). For example, the key types of personal data we hold include:

1.3.1 **Contact details** such as names, email addresses, residential address;

1.3.2 **Occupational details** such as occupation and year of retirement;

1.3.3 **Financial details** such as details of savings, expenses and sources of income;

1.3.4 **Medical records** such as details of disabilities and the name of G.P.;

1.3.5 **Personnel records** such as HR records for the Trust Administrator and Trustee details.

1.4 This policy is designed to establish processes for ensuring the security of personal data and to establish administrative, technical, and physical safeguards to protect against unauthorised access or use of this information.

2. Status of this policy

2.1 A failure to comply with this policy could expose the Trust to enforcement action, including fines, by the Information Commissioner's Office ("**the ICO**") and/or by individuals who suffer damage as a result.

There is also a risk of very damaging negative publicity for the Trust if any breach is made public. It is therefore important that this policy is complied with by all Trustees and The Trust Administrator

2.2 This policy does not form part of any employee's formal contract for services. However, it is a condition for services that the Trust Administrator will abide by the rules and policies made by the Trust from time to time and that includes this policy, and failure to comply with this policy could amount to misconduct, which is a disciplinary matter. In the case of trustees this policy may result in the termination of the trusteeship.

3. Security measures and procedures

All Trustees and The Trust Administrator must comply with the following procedures when dealing with personal data:

Physical entry controls

3.1 Desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential);

Data storage

3.2 Personal data about grant applicants, beneficiaries, staff, trustees and organisational contacts should usually only be stored [centrally on the Trust's database which has appropriate security protections in place];

3.3 Access to the personal data on the Trust's database or held elsewhere should be limited only to The Trust Administrator who need access to it as part of their role at the Trust;

3.4 Back-ups are made of the personal data held on the Trust's database on a [nightly/weekly] basis. Personal data held on other devices should be backed-up regularly;

Paper records

3.5 Paper records containing personal data must be kept securely in the Administrator's office or archive cupboard at St Mary's CE Primary School. These are locations which are locked when not in use;

Any paper records containing personal data relating to the recruitment and employment of the Trust's employees must be stored securely.

Electronic records

3.6 The Trust Administrator and Trustees should not share their password with anyone. Passwords should include a mixture of letters and

numbers; passwords which are easy to guess (such as a name or date of birth) should be avoided;

3.7 The Trust Administrator should lock her PC screens when they are left unattended, and ensure that when their screens are displaying confidential information,

3.8 When the Trust Administrator or Trustees cease to be engaged with the Trust, all of their files, records and computer equipment belonging to the Trust must be returned and their passwords must be changed;

Data disposal

3.9 Paper files containing personal data which are no longer required should be shredded using shredding machines. Where such files are recycled, only reputable companies who have given appropriate security undertakings should be used;

3.10 When laptop or computer hard drives, USB drives, or other electronic equipment which may contain personal data, are no longer required, they should be disposed of either through using software to 'wipe' the hard drive, or through mechanical means which renders the personal data inaccessible.

Travelling with personal data

3.11 Data users must keep personal data secure when travelling or using it outside the Trust's offices. For instance, documents and laptops must be kept secure and not left accessible by others. Computers, laptops, mobile phones and PDAs must be locked when not in use, with screen locks enabled if left unattended;

3.12 Personal data should not be downloaded to mobile devices such as laptops, PDAs and USB sticks unless absolutely necessary. Access to such data must be password protected and then deleted immediately after use;

Sending personal data

3.13 When sending personal data by post, you should use registered post or courier. Do not send CDs or memory sticks containing personal data by ordinary post, and encrypt or password-protect any CDs or memory sticks which are sent;

3.14 Any request for personal data to be emailed must be appropriately authenticated. Personal data sent by email should be sent using password-protected files, and where sensitive personal data, financial information, or any other personal data which might cause distress or damage if mislaid, wrongly directed or compromised is being sent,

consideration should be given as to whether there is a more secure method of transmitting the information (for example, using encryption);

4. Sharing personal data with third parties

4.1 Personal data should not be shared with third parties, whether those parties are acting on Trust's behalf or using the personal data for their own purposes, without first ensuring that appropriate care will be taken in relation to the personal data.

4.2 Where a request for information is received from a third party, you should be careful about disclosing any personal data held by the Trust. In particular you should:

4.2.1 Check the identity of the person making the enquiry and whether they are entitled to receive the information they have requested.

4.2.2 Require the third party to put their request in writing so the third party's identity and entitlement to the information may be verified.

4.2.3 Refer to the Trust Administrator for assistance in difficult situations.

5. Monitoring and review of the policy

5.1 The Trust Administrator is responsible for ensuring compliance with the Act and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Trust Administrator

5.2 This policy is reviewed on an annual basis by our board of trustees to ensure it is achieving its stated objectives, and may be amended from time to time to reflect any changes in legislation or internal policy decisions.

6. Data security breaches

6.1 If you become aware of any security breach in relation to the Trust's personal data for example unauthorised access to, theft of, or loss of any personal data you must report the incident to the Trust Administrator immediately.

6.2 Any security breach in relation to the Trust's personal data will be reported to the trustees and an assessment will be carried out as soon as practicable by management staff and/or the trustees as appropriate to determine how to deal with the breach, including considering the following matters:

6.2.1 the facts of the breach and any necessary investigation;

6.2.2 any action which can be taken to stop or mitigate the breach;

6.2.3 who, if anyone, should be notified of the breach, including but not limited to the ICO and any individuals whose personal data is the subject of the breach;

6.2.4 whether the breach was caused by a third party processing personal data and if so what contractual agreement the Trust has in place with that party;

6.2.5 if the breach was caused by an Trustee or the Trust Administrator whether any disciplinary or other action is appropriate; and

6.2.6 what improvements can be made to the Trust's procedures in order to ensure the breach does not re-occur.

THE GREIG TRUST

Incorporating

THE HS & SV AND D & M GREIG FUNDS
THE DAVID GREIG EDUCATIONAL TRUST

DATA COLLECTION STATEMENTS

The following statements have been added to application and monitoring foms of The Greig Trust to comply the Data Protection Act 1998.

Application Form for Schools/Organisations

The Greig Trust will use the personal information about any individual contacts/referrers provided in this form and elsewhere to administer the application and monitoring process and any grant which is awarded.

Monitoring Form for Schools/Organisations

The Greig Trust will use the personal information about any individual contacts provided in this form and elsewhere to administer the monitoring process in relation to the grant.

Application Form for Individuals

The Greig Trust ("the Trust") will use the personal information about the applicant and other individuals which are provided on this form and elsewhere to administer the application and monitoring process and any grant which is awarded. Such personal information may be shared with the organisation which has referred the applicant to the Trust to provide confirmation of the outcome. The Trust may also seek consent from the applicant to share the personal information with other organisations and persons whom the Trust considers may be able to assist the applicant.

The information collected may include sensitive personal information such as details of the applicant's disabilities or health conditions, and by submitting this form the applicant confirms that they are happy for the Trust to use such information as described above.

All individuals named in this form must be provided with the information above and must agree to the submission of this application. Wherever possible, the applicant should sign at the end of this form to confirm their agreement, and that of any other individuals named in this form, to this application. If you are submitting this form without the applicant's signature, you confirm that the applicant and any other individuals named in this form have been provided with the information above and have consented to the submission of this application.