GREENFIELDS EDUCATIONAL TRUST
GENERAL DATA PROTECTION POLICY
(Issued 22nd May 2018)

1.0 POLICY STATEMENT AND PRINCIPLES:

1.1 The Data Protection Act 1998 protects an individual's rights in the context of their information. Greenfields Educational Trust's organisations (hereafter known at the "Trust") process large amounts of personal data about members of the Trust community. Under the Data Protection Act, the Trust must process such personal data fairly. This includes telling pupils and parents how their personal data will be held and used by the Trust. This Data Protection Policy is intended to help meet that legal requirement. It should be noted that data protection should always take second place to safeguarding and child protection. If there is a potential conflict between the two competing requirements, the welfare of the child is paramount.

1.2 This policy is intended to provide information about how the Trust will use or process personal data about individuals including current, past and prospective pupils; and their parents, carers or guardians (referred to in this policy as "parents"), staff and visitors. It applies in addition to any of the Trust's terms and conditions, and any other information they may provide about a particular use of personal data. The General Data Protection Regulation (GDPR) is an EU Regulation which was to replace the current Directive and be directly applicable in all Member States without the need for implementing national legislation. It is to be adopted by the EU on 25 May 2018.

1.3 Anyone who works for, or acts on behalf of, the Trust (including staff, volunteers, trustees and service providers) should also be aware of and comply with this Data Protection Policy, which also provides further information about how personal data about those individuals will be used. Further details are in Section 3 and 4 of this policy.

1.4 The Trust is required to notify the Information Commissioner (ICO) of the processing of personal data. This information will be included in a public register which is available on the ICO website.

1.5 In accordance with the Data Protection Act 1998, the Trust has notified the Information Commissioner's Office of its processing activities. The Trust's ICO registration number is Z1062897 and its registered address is Greenfields Educational Trust, Priory Road, Forest Row, East Sussex, RH18 5JD.

1.6 Greenfields Educational Trust, as a corporate body, is named as the Data Controller for the Trust under the Act as it holds and uses personal information. It decides how and why the information is used and has a responsibility to establish workplace practices and policies that are in line with the Act.

1.7 As Data Controller, Greenfields Educational Trust must therefore:
• Manage and process personal data properly
• Protect the individual's right to privacy
• Provide an individual with access to all personal data held on them.

1.8 The Trust has appointed the Bursar as Data Protection Officer ("DPO") who will endeavour to ensure that all personal data is processed in compliance with this policy and the Act.

1.9 'Personal data' relates to a living individual and allows that individual to be identified from it (either on its own or along with other information likely to come into the organisation's possession).

1.10 Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:
• used fairly and lawfully
• used for limited, specifically stated purposes
• used in a way that is adequate, relevant and not excessive
• accurate
• kept for no longer than is absolutely necessary
• handled according to people's data protection rights
• kept safe and secure
• not transferred outside the UK without adequate protection.

1.11 Greenfields Educational Trust is committed to maintaining these principles at all times. This means that the Trust will:
• Inform the people whose data is being stored (so-called 'Data Subjects'), why the Trust needs their personal information, how they will use it and with whom it may be shared. This is known as a 'Privacy Notice'
• Check the quality and accuracy of the information held
• Apply the records management policies and procedures to ensure that information is not held longer than is necessary (either until a former pupil's 25th birthday, or longer in the case of Child Protection files)
• Reserve the right to keep data on Alumni where their permission has been received
• Ensure that when information is authorised for disposal it is done appropriately
• Ensure that appropriate security measures are in place to safeguard personal information whether it is held in paper files or on a computer system
• Only share personal information with others when it is necessary and legally appropriate to do so
• Set out clear procedures for responding to requests for access to personal information known as 'Subject Access Request' in the Data Protection Act 1998
• Train all staff so that they are aware of their responsibilities and of the Trust's relevant policies and procedures.

2.0 TYPES OF DATA THAT ARE MANAGED BY THE SCHOOL:

2.1 The Trust may process a wide range of personal data about individuals including current, past and prospective pupils and their parents as part of its operation, including by way of example:

- Names, addresses, telephone numbers, e-mail addresses and other contact details
- Car details about those who use the Trust's car parking facilities
- Bank details and other financial information, e.g. about parents who pay fees to the school or payroll details for members of staff
- Past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), examination scripts and marks
- Information about individuals' health, and contact details for their next of kin
- References given or received by the school about pupils and staff, and information (such as details on safeguarding concerns) provided by previous educational establishments and/or other professionals or organisations working with pupils
- Images of pupils (and occasionally other individuals) engaging in school activities, and images captured by the school's CCTV system (in accordance with the Trust's CCTV policy on taking, storing and using images of children).

2.2 The Trust usually receives personal data from the individual directly (or, in the case of pupils, from parents). However, in some cases personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual), or collected from publicly available resources.

2.3 The Trust may, from time to time, need to process sensitive personal data regarding individuals. This type of data could include information about an individual's physical or mental health, race or ethnic origin, political or religious beliefs, sex life, trade union membership or criminal records and proceedings. Sensitive personal data is entitled to special protection under the Act, and will only be processed by the school with the explicit consent of the appropriate individual, or as otherwise permitted by the Act.

2.4 As part of its operations, the Trust will use (and where appropriate share with third parties) personal data about individuals for a number of purposes, including:

- For the purposes of pupil selection and to confirm the identity of prospective pupils and their parents
- To provide education services (including SEND support), careers advice and extra-curricular activities to pupils; to monitor pupils' progress and educational needs; and maintain relationships with alumni and the Trust's community
- For the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor educational performance
- To give and receive information and references about past, current and prospective pupils, (including data relating to outstanding fees or payment

history) to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils

- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the school
- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to organisers of educational trips or holiday clubs
- To monitor (as appropriate) use of the Trust's IT and communications systems in accordance with the Trust's IT acceptable use policies
- To make use of photographic images of pupils in Trust publications, websites and (where appropriate), on the social media channels in accordance with the Trust's policy on taking, storing and using images of children
- For security purposes, and for regulatory and legal purposes (for example child protection and health and safety) and to comply with its legal obligations
- Where otherwise reasonably necessary for the Trust's purposes, including to obtain appropriate professional advice and insurance for the Trust's organisations.

3.0 DATA ACCURACY AND SECURITY:

3.1 The Trust will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must notify the DPO of any changes to information held about them.

3.2 An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act) and may do so by contacting the DPO in writing.

3.3 The Trust will take appropriate technical and organisational steps to ensure the security of personal data about individuals, ensuring that it is held in accordance with the Principles of the Act. All staff will be made aware of this policy and their duties under the Act

4.0 SAFEGUARDING PRACTICE and INFORMATION SHARING:

4.1 Whilst the Data Protection Act places duties on organisations and individuals to process personal information fairly and lawfully, it is not a barrier to sharing information where the failure to do so would result in a child or vulnerable adult being placed at risk of harm.

4.2 Human rights concerns, such as respecting the right to a private and family life would not prevent sharing where there are real safeguarding concerns. For further information, see HM Government's "Information sharing:

Advice for practitioners providing safeguarding services to children, young people, parents and carers" (March 2015).

4.3 The Local Safeguarding Children Board (LSCB) can require an individual or body to comply with a request for information, as outlined in section 14B of the Children Act 2004. This can only take place when the information requested is for the purpose of enabling or assisting the LSCB to perform its functions. Any request for information about individuals should be necessary and proportionate to the reason for the request and should be made to Designated Safeguarding Leads or Safeguarding Coordinator who must discuss any such request with the Data Protection Officer.

5.0 RIGHTS OF ACCESS TO PERSONAL DATA ('SUBJECT ACCESS REQUEST'):

5.1 Individuals have the right under the Act to access personal data about them held by the school, subject to certain exemptions and limitations set out in the Act. Any individual wishing to access their personal data should put their request in writing to the DPO

- Information about a child may be released to a person with parental responsibility, although the best interests of the child will also be taken into consideration. The child in question needs to be mature enough to understand their rights.
- Pupils aged 12 or over are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested. All subject access requests from pupils will therefore be considered on a case-by-case basis.

5.2 Parents should be aware that in certain situations they may not be consulted. In general, the Trust will assume pupils consent to disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the school's opinion, there is a good reason to do otherwise.

5.3 However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the Trust will maintain confidentiality unless, in the Trust's opinion, there is a good reason to do otherwise; for example, where the school believes disclosure will be in the best interests of the pupil or other pupils.

5.4 The ICO states that 'if the organisation is confident that the child can understand their rights, then it will respond to the child rather than the parent. What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so.' (ICO: Find out how to request your personal information')

5.5 The Trust will endeavour to respond to any such written requests (known as "subject access requests") as soon as is reasonably practicable and in any event within the statutory time-limit of 30 calendar days from the date of receiving the Subject Access Request. According to the Information Commissioner's Office guidelines, the request may incur a charge.

5.6 If an individual believes that any information held on him or her is incorrect or incomplete, then they should write to the DPO as soon as possible. The Trust will promptly correct any information found to be incorrect.

5.7 Information which an individual is entitled to access:

- Whether any data is being processed on the particular individual
- A description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people
- A copy of the personal data held
- Details about the source of the data 'Subject access provides a right for the requester to see their own personal data rather than a right to see copies of documents that contain their personal data. An organisation may choose to provide photocopies of original documents, but is not obliged to do so'. (ICO SAR Code of Practice Version 1.2 p8)

5.8 Exemptions

- All members of the Trust community should be aware that certain data is exempt from the right of access under the Act. This may include information which identifies other individuals, or information which is subject to legal professional privilege.
- The Trust is also not required to disclose any pupil examination scripts (though examiners' comments may, in certain circumstances, be disclosed), nor any reference given by the school for the purposes of the education, training or employment of any individual.

6.0 DATA PROTECTION FOR STAFF:

The following Data Protection Code of Conduct should be adhered to at all times:

- Staff should only ever share information on a need to know basis
- Data protection should never be used as an excuse for not sharing information where necessary; the welfare of the child is paramount
- Seniority does not give an automatic right to information
- All emails are discloseable, less a few exemptions
- Only keep data for as long as is necessary (see Retention tables in Appendices A & B).

7.0 CONFIDENTIALITY:

7.1 Any Trust information/records including details of pupils, parents and employees whether actual, potential or past, other than those contained in authorised and publicly available documents, must be kept confidential unless

the Trust's prior written consent has been obtained. This requirement exists both during and after employment, and relates in particular to any information used for the benefit of any future employer.

7.2 The law states that where a teacher/tutor is facing an allegation of a criminal offence involving a pupil registered under the Trust, the teacher/tutor concerned is entitled to anonymity until they are either charged with an offence or the anonymity is waived by them. If publication is made on behalf of the Trust, the Trust, including the Senior of the organisation involved, and Trustees could be prosecuted.

7.3 If a teacher/tutor is charged with such an offence, all communication must be directed through the appropriate head of the organisation involved, who will have authority to deal with the allegation and any enquiries to ensure that this restriction is not breached. If a member of staff is found to have breached (whether intentionally or otherwise) this duty, any accusations will be dealt with under the Trust's Disciplinary Procedure.

8.0 OFF-SITE ACCESS TO PERSONAL DATA:

8.1 The Trust must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data.

8.2 The Trust is expected to ensure that measures are taken to avoid the accidental loss of, or damage to, personal data. This is in relation to data belonging to all members of the Trust community.

8.3 ENGAGE, the Trust's data management system, may be used on personal devices provided that the device is secure and password protected.

8.4 For pupils on residential trips, medical information and other relevant information (e.g. passport details) may be taken off site by the trip leader but must be carefully managed and kept securely.

9.0 USE OF PHOTOGRAPHS:

The Data Protection Act is unlikely to apply in many cases where photographs are taken in schools and other educational institutions. Fear of breaching the provisions of the Act should not be wrongly used to stop people taking photographs or videos. Where the Act does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.

- Photos taken for official Trust use may be covered by the Act and pupils and students should be advised why they are being taken.
- Photos taken purely for personal use are exempt from the Act. However, please see the guidance given in the Greenfields Trust Staff Code of Conduct and EYFS Social Media Policy
- Photographs of pupils or students are taken for ENGAGE. These images are stored electronically with other personal data and the terms of the Act will apply

• Photographs taken for Trust websites, prospectuses or social media feeds are classed as personal data but will not breach the Act as long as the children and/or their parents are aware this is happening and the context in which the photo will be used
• Parental permission is sought through the Use of Photographs Form at registration. Parents are given information about the types of uses made of the pupils' photographs, and are given the option to opt out. The names of pupils who are not allowed to feature in published photographs are made available to staff.

10.0 WHAT TO DO IN THE EVENT OF A SUSPECTED DATA BREACH:

10.1 A personal data breach is "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 in connection with the provision of a public electronic communications service" (Data Breach Notification under the GDPR: Issues to Consider: Browne Jacobson LLP).

10.2 A personal data breach may mean that someone other than the Trust gets unauthorised access to personal data. But a personal data breach can also occur if there is unauthorised access within the Trust or if a member of staff accidentally alters or deletes personal data.

10.3 In the event of a breach, the member of staff must notify the Data Protection Officer within 24 hours of becoming aware of the breach. This notification must include at least:
• The member of staff's name and contact details
• The date and time of the breach (or an estimate)
• The date and time that the breach was detected it
• Basic information about the type of breach
• Basic information about the personal data concerned.

10.4 The DPO will then make a judgement on the best course of action which is likely to include notifying the senior of the organisation involved, and the Designated Safeguarding Lead, in the event that the data breach includes pupils' details, as appropriate.

11.0 DATA PROTECTION FOR PUPILS AND FAMILIES:

11.1 The Trust will use the contact details of parents, alumni and other members of the Trust's community to keep them updated about the activities of the community, including sending updates and newsletters, by email and by post.

11.2 With permission from the relevant individual, the Trust may also:

• Share personal data about parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships with the school community, such as the Parent Teacher's Association.

• Contact parents and/or alumni by post and email in order to promote the Trust and raise funds for it.

11.3 If any member of the Trust community wishes to limit or object to any such use, or would like further information about them, they should contact the DPO in writing.

11.4 Pupils are required to respect the personal data and privacy of others, and to comply with the Trust's IT Acceptable Use Policy and other relevant Trust regulations.

12.0 QUERIES AND COMPLAINTS:

12.1 Any comments or queries on this policy should be directed to the DPO using the following contact details: Mrs Angela Lockey, Data Protection Officer, Greenfields Educational Trust, Priory Road, Forest Row, East Sussex, RH18 5JD.

12.2 If an individual believes that the Trust has not complied with this policy or acted otherwise than in accordance with the Act, they should utilise the Trust's Complaints Procedure and should also notify the DPO.

13.0 DATA RETENTION AND STORAGE GUIDELINES:

13.1 In these guidelines, "record" means any document or item of data which contains evidence or information relating to the Trust, its staff or pupils. Some of this material will contain personal data of individuals as defined in the Act, but not all.

13.2 Many, if not most, new and recent records will be created, received and stored electronically. Others (such as Certificates, Registers or older records) will be original paper documents. The format of the record is less important than its contents and the purpose for keeping it.

14.0 PUPIL RECORDS:

14.1 Guidance on maintaining pupil records can be found in the IRMS Information Management Toolkit for Schools 2016 and information described in this section is kept by Greenfields Educational Trust.

14.2 These guidelines apply to information created and stored in both physical and electronic format. The pupil record starts its life when a file is opened for each new pupil as they begin their education. This is the file which will follow the pupil for the rest of his/her school/educational career.

14.3 If pre-printed file covers are not being used then the following information should appear on the front of the paper file:
• Surname
• Forename
• DOB

14.4 Inside the pupil's folder the following information should be easily accessible:

- The name of the pupil's doctor
- Emergency contact details
- Gender
- Preferred name
- Position in family
- Ethnic origin
- Language spoken at home (if other than English)
- Religion
- Any allergies or other medical conditions that it is important to be aware of
- Names of adults who hold parental responsibility with home address and telephone numbers
- Numbers of any additional relevant carers and their relationship to the child
- Name of the Trust, date of admission
- Date of leaving
- Any other agency involvement e.g. speech and language therapist, paediatrician.

14.5 Other items which should be included in the pupil record:

- If the pupil has attended an early years setting, then the record of transfer should be included on the pupil file
- Admission form (application form)
- Most recent Privacy Notice
- Photography Consents
- Any information relating to a major incident involving the child (either an accident or other incident)
- Any reports written about the child
- Any information about a statement and support offered in relation to the statement
- Any relevant medical information (should be stored in the file in a sealed envelope clearly marked as such or in a separate medical file)
- Child protection reports/disclosures (should be stored in a separate file with a sticker on the front to indicate that there is another CP file on that child)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil.

14.6 The following records are subject to shorter retention periods and do not need to be transferred to the pupil's next school:

- Absence notes
- Parental consent forms for trips/outings (in the event of a major incident the parental consent forms should be retained with the incident report not in the pupil record)
- Correspondence with parents about minor issues

• Accident forms (these should be stored separately and retained on the Trust premises until their statutory retention period is reached. A copy could be placed on the pupil file in the event of a major incident).

15.0 TRANSFERRING THE PUPIL RECORD TO ANOTHER SCHOOL:

15.1 The pupil record should not be weeded before transfer to another school unless any records with a short retention period have been placed in the file. It is important to remember that the information which may seem unnecessary to the person weeding the file may be a vital piece of information required at a later stage.

15.2 The Trust does not need to keep copies of any records in the pupil record except if there is an ongoing legal action when the pupil leaves the school. Custody of and responsibility for the records passes to the school the pupil transfers to.

15.3 Files should not be sent by post unless absolutely necessary. If this does need to happen, then files should be sent by registered post with an accompanying list of the files included in the parcel. The new school should sign the enclosed form to say that they have received the files and return the form to Trust organisation that sent them. Where appropriate, records can be delivered by hand with signed confirmation for tracking and auditing purposes.

15.4 Electronic documents (including Safeguarding information, where relevant) that relate to the pupil file also need to be transferred, or, if duplicated in a master paper file, destroyed.

16.0 STORAGE OF RECORDS:

16.1 All pupil records should be kept securely at all times. Paper records, for example, should be kept in lockable storage areas with restricted access, and the contents should be secure within the file. Equally, electronic records should have appropriate security. Access arrangements for pupil records should ensure that confidentiality is maintained whilst equally enabling information to be shared lawfully and appropriately, and to be accessible for those authorised to see it.

16.2 In order to mitigate against the loss of electronic information, the Trust operates a back-up system for all information held electronically to enable the restoration of the data in the event of an environmental or data corruption incident.

16.3 Digital Records

• Digital records can be lost or misappropriated in huge quantities very quickly. Access to sensitive data - or any large quantity of data – should as a minimum be password-protected and held on a limited number of devices

only, with passwords provided on a need-to-know basis and regularly changed

• Personal information should not be stored on the hard drive of any laptop or PC unless the device is running encryption software. Staff are advised not to hold personal information about students or other staff on mobile storage devices including memory sticks, phones, tablets, portable hard drives or even on CDs

• The Trust asks students and staff to change their passwords on a termly basis. Password sharing is strongly discouraged and alternative ways of sharing data are used such as shared Google Drive

• Emails, whether they are retained electronically or printed out as part of a paper file are also "records" and may be particularly important: whether as disclosable documents in any litigation, or as representing personal data of the sender (or subject) for data protection/data privacy purposes. Again, however, the format is secondary to the content and the purpose of keeping the document as a record

• It is important that all staff bear in mind, when creating documents and records of any sort (and particularly email), that at some point in the future those documents and records could be disclosed – whether as a result of litigation or investigation, or because of a Subject Access Request under the Act. It is therefore crucial that all documents are accurate, professional and as objective as possible.

16.4 Paper records

• Under the Act, paper records are only classed as personal data if held in a "relevant filing system" – i.e. one that is organised, and/or indexed, so that specific categories of personal information relating to a certain individual are readily accessible, and thus searchable as a digital database might be. An example of this could be an alphabetical personnel file split into marked dividers which would fall under this category, but a merely chronological file of correspondence may well not.

• However, when personal information is contained on print-outs taken from electronic files, this data has already been processed by the Trust and falls under the Act.

17.0 THE ARCHIVING AND ERASURE OF RECORDS:

Staff given specific responsibility for the management of records must ensure the following as a minimum:

• Records – whether electronic or hard copy – should be stored securely, encrypted if possible, so that access is available only to authorised persons and the records themselves are available when required and (where necessary) searchable

• Important records, and large or sensitive personal databases should not be taken home or – in the case of digital data – carried or kept on portable devices (whether memory sticks, mobile phones or other electronic equipment) unless absolutely necessary

• Issues of back-up or migration are approached in line with general Trust policy (such as professional storage solutions or IT systems) and not individual ad hoc action.
• Arrangements with external storage providers – whether physical or electronic (in any form, but particularly "cloud-based" storage) – must be supported by robust contractual arrangements providing for security and access
• Reviews must be conducted on a regular basis in line with the guidance on suggested retention periods, to ensure that all information being kept is still relevant and (in the case of personal data) necessary for the purposes for which it is held
• The destruction or permanent erasure of records, if undertaken by a third party, must be carried out securely – with no risk of the re-use, disclosure or re-construction of any records or the information contained in them
• For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed
• Paper records should be shredded using a cross-cutting shredder; CDs / DVDs / discs should be cut into pieces. Hard-copy images, AV recordings and hard drives should be dismantled and destroyed and old PCs must be wiped clean
• Where third party disposal experts are used they should ideally be supervised but, in any event, under adequate contractual obligations to the Trust to process and dispose of the information securely

18.0 RELATED POLICIES:

• Admissions
• Attendance and Registers
• Behaviour Management
• CCTV
• Complaints
• Computer Usage
• Disability
• Educational Visits
• Equal Opportunity and Racial Equality
• Social Media and E-Safety
• Exclusion
• First Aid
• Health & Safety
• Risk Assessment
• Safe Staff Recruitment
• Safeguarding & Child Protection
• SEND Policy (including the Accessibility Plan)
• Staff Conduct and Whistleblowing Policy

Policy compiled by Jeff Smith – Executive Head, for Greenfields Educational Trust, 22nd May 2018. Reviewed 25th May 2018 Trust Management.