BENEDETTI
FOUNDATION

Data Protection Policies and Procedures

LAST UPDATED: 13.2.21
REVIEW DUE BY BOARD: MARCH 2021

Data Protection Policy

1.0 Context

The Benedetti Foundation is a charity (registered in Scotland SRCN SC049688) that promotes music and musical education by organising or supporting workshops for music teachers and young musicians across the United Kingdom.

It is a data controller and responsible for your personal data, and is referred to as 'BF', 'we', 'us' or 'our' in this notice and policy.

BF is committed to being transparent about how it collects and uses personal data, and to meeting its data protection obligations in accordance with the General Data Protection Regulations (GDPR) as enacted by the UK Data Protection Act 2018. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of trustees, employees, contractors, job applicants, volunteers and supporters, teachers, ambassadors, parents and children and others associated with BF and its activities. It also applies to former members of each of these categories. These are referred to in this policy as relevant individuals.

This policy is not contractual but indicates how BF intends to meet its legal responsibilities for data protection. We reserve the right to vary, replace or withdraw this policy at any time.

It is important that the personal data we hold about you is accurate and current. We ask all relevant individuals to keep us informed if their personal data change during their relationship with us.

Contact details for data protection purposes

Data officer: Laura Gardiner, Foundation Director

This person is responsible for data protection compliance at BF and may be contacted as follows:

The Benedetti Foundation
c/o Turcan Connell
Princes Exchange
1 Earl Grey Street

Edinburgh
EH3 9EE

Email: laura@benedettifoundation.org
Website: http://www.benedettifoundation.org

ICO Registration Number: ZA674093

All relevant individuals have the right to make a complaint at any time to:

- the Information Commissioner's Office – Scotland scotland@ico.org.uk, or
- the Information Commissioner's Office (England and Wales) (www.ico.org.uk)

who collectively are the UK's supervisory authority for data protection issues.

We would however appreciate the chance to deal with your concerns before you approach the ICO, so please contact us in the first instance.

2.0 Definitions

This is what some of the key terms used in this policy mean:

Personal data is any information that relates to an individual who can be directly or indirectly identified from that information.

Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

Special categories of personal data means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric and genetic data (where used for ID purposes).

3.0 Data protection principles

BF strives to ensure that its use of personal data meets the the following data protection principles:

- Personal data is processed lawfully, fairly and in a transparent manner
- Personal data is collected only for specified, explicit and legitimate purposes
- Personal data is processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- Personal data is accurate, and all reasonable steps are taken to ensure that inaccurate personal data is rectified or deleted without delay
- Personal data is kept only for the period necessary for processing
- Appropriate measures are adopted to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

BF endeavours to explain to all relevant individuals the reasons for processing their personal data, how we use such data and the legal basis for processing in our privacy notices. Personal data of relevant individuals will not be processed for other reasons.

BF will take all reasonable steps to update personal data promptly if a relevant individual advises that their information has changed or is inaccurate.
BF will endeavour to keep a record of its processing activities in respect of personal data in accordance with the requirements of the GDPR.

4.0 Types of data held

Personal data gathered during the recruitment, working, volunteering, teaching or ambassadorial relationship with BF, or that gathered from trustees during their trusteeship, or from parents and children in the course of registering for and attending BF sessions and activities is held wherever possible in electronic format. Occasionally there are legitimate business reasons for paper records to be held in addition or instead of the electronic version, but BF strives to keep these to a minimum.

The following types of data may be held by BF as appropriate, on relevant individuals. This is not an exhaustive list, nor does it indicate that every type of data listed is held in respect of every person:

- Name, address, phone numbers, email addresses, marital status, date of birth and gender
- Name of child, relationship to child, child's name, date of birth, school attended, level of musical attainment, teacher, instrument, siblings
- Health and wellbeing data relating to a child attending a BF session or activity
- Application forms and other information gathered during recruitment and selection procedures
- Identity checks, including entitlement to work in the UK
- Disclosure and Barring Service (DBS) checks and supporting information
- References from former employers, education establishments and/or personal referees, data relating to suitability to teach or assume an ambassadorial role, data relating to suitability for trusteeship
- Data relating to donations made to BF and Gift Aid
- National Insurance numbers
- Tax codes
- Job title, job description and pay details
- Bank account information
- Terms and conditions of employment
- Conduct and/or capability issues such as letters of concern, improvement notes, disciplinary proceedings
- Holiday and sickness absence records
- Performance management information, such as supervision notes, appraisals, performance development plans and training records

5.0 Individual rights

As data subjects, relevant individuals have a number of rights in relation to their personal data.

Relevant individuals have the right to be informed about how BF processes personal data about them and the reasons for processing. BF privacy notices explain what data we collect, how we collect and process it and the lawful bases relied on for processing.

If BF intends to use data already collected for a different reason than that already communicated, we will do our best to inform relevant individuals of the new reason in advance.

5.1 Subject Access Requests (SAR)

Relevant individuals have the right to access the personal data held on them by BF.

To make a SAR, the relevant individual should consult https://ico.org.uk/your-data-matters/your-right-of-access/, complete a SAR form and send it to BF's Data Officer using the contact details at the start of this policy. Please ensure specific details of the data being requested are included to allow us to respond as efficiently as possible.

When we receive a SAR form, we may ask for proof of identification before the request can be processed. We will always ask for this proof if the SAR relates to a child's data.

BF's Data Officer will then confirm:

- whether or not the relevant individual's data is processed and if so why; the categories of personal data concerned and the source of the data if it is not collected from the relevant individual
- to whom the relevant individual's data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers
- for how long the relevant individual's personal data is stored (or how that period is decided)
- the relevant individual's rights to rectification or erasure of data, or to restrict or object to processing
- the relevant individual's right to complain to the Information Commissioner if they think BF has failed to comply with their data protection rights; and
- whether or not BF carries out automated decision-making and the logic involved in any such decision-making

BF's Data Officer will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless agreed otherwise.

BF will endeavour to respond to a subject access request within one month of receipt unless a large amount of data is involved.

We may be unable to supply certain pieces of information, for instance where it is subject to legal privilege. Where this is the case, BF's Data Officer will write to the individual to inform them that the request cannot be compiled with, and give an explanation for the reason.

If a subject access request is manifestly unfounded, excessive, or repetitive BF is not obliged to comply with it.

Relevant individuals must inform BF's Data Officer immediately if they believe any data held on them is inaccurate, whether or not this comes to light through a SAR.

In the event that inaccurate data was disclosed to third parties, we will inform the third party of the correction where possible, and also inform the individual of the third parties to whom the data was disclosed.

5.2 Other rights

Relevant individuals have a number of other rights in relation to their personal data.

They can require BF to stop processing or erase data:

- that is no longer necessary for the purposes it was processed
- if the interests of the individual override BF's legitimate grounds for processing data (where BF relies on its legitimate interests as a reason for processing data)
- if the processing is unlawful
- if the data is inaccurate

To ask for any of these steps to be taken, the individual should send their request to BF's Data Officer. If the response is that BF will take no action, this will be confirmed to the individual in writing.

6.0 Data security

BF takes the security of personal data seriously. We strive to follow the following practices and controls so we can protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is only accessed by BF personnel in the proper performance of their duties.

- personal data (sensitive or not) will only be recorded where it is strictly necessary for the effective running of BF and its charitable activities
- if data is not relevant or needed for the specific purpose for which it is collected, or if it is out of date, or if it sis no longer needed it will not be recorded or processed
- electronic and paper files will be reviewed and purged at regular intervals in accordance with our data retention protocols
- we will use electronic files over paper files wherever possible. All files or written information of a confidential nature will be stored securely and only seen by people who have a legitimate need or right to access them
- all appropriate care will be taken to ensure that data entered onto electronic files at BF is accurate
- passwords and user IDs will be kept confidential and unshared, and changed on a regular basis
- any personal data which must of operational necessity be transported to BF sessions or events (for example on a laptop) will be password protected and secured at all times
- all BF trustees, staff, contractors, volunteers, teachers and ambassadors will read and confirm they have understood BF's Data Breach policy, and will undertake fully to comply with preventative measures in the course of their BF duties
- Where BF engages third parties to process personal data on its behalf, BF will endeavour to ensure that they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data they receive

7.0 Privacy Impact Assessments

If any data processing BF intends to carry out might result in a high risk to individual's rights and freedoms, a Privacy Impact Assessment (PIA) will be made to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

8.0 Data breaches

BF maintains a separate Data Breach policy, which is reviewed annually.

9.0 International data transfers

In the course of its operations, BF may process and/or store personal data using third party data controller/processors which have some or all of their operations based outside of the EA. Examples include Dropbox and PayPal. BF is not accordingly, able to offer assurance that personal data processed by such authorised third parties is not transferred outside of the EA, nor that the standard of any such processing is at least equivalent to that required under GDPR. Data subjects are however reminded that in is in the commercial interested of these third parties to ensure that personal data is handled securely and appropriately, and that in each instance they assert that they comply with the EU-US Privacy Shield Frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union.

10.0 Automated decision making

Individuals have the right not to have decisions made about them solely on the basis of automated decision making processes. BF does not make any decisions based on such processes.

11.0 Individual responsibilities

Individuals are responsible for helping BF keep their personal data up to date. Individuals who are associated with BF operationally should let the Data Officer or other appropriate officer know if their data changes – for example if they move house or change bank details.

Trustees, employees, contractors, volunteers and supporters, teachers, and ambassadors may have access to the personal data of other individuals such as parents and children in the course of their working with BF. All are responsible for upholding the data protection principles in this policy, and for meeting our data protection obligations to those supported by the charity.

We are all responsible for making sure that:

- we only access data we have authority to access, and only do so for legitimate and authorised purposes
- we only disclose data to individuals (whether inside or outside the organisation) who have appropriate authorisation and a legitimate need to see them
- we keep data secure (for example by complying with guidance and protocols on using databases, computers, passwords, secure file storage and organising timely destruction of data)
- where it is operationally necessary to transport data to BF sessions or events, for example on a laptop, the data will be protected by appropriate security measures (password protection, encryption) and kept secure at all times
- we do not store personal data on local drives or on personal devices that are used for work purposes

Failing to observe these requirements may amount to a disciplinary offence. Significant or deliberate breaches of this policy may constitute gross misconduct and could lead to summary dismissal.

12.0 Training

BF will provide training to all individuals about their data protection responsibilities.

BF will strive to ensure that data protection principles are integrated into the design of new activities and processes over time.

13.0 Implementation, monitoring and review of this policy

BF's Data Officer has overall responsibility for implementing and monitoring this policy, and providing updates whenever there are relevant changes in legislation or working practices at BF.

The policy will be reviewed annually by the BF Board.

Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Data Officer. Any associates of BF who considers that the policy has been breached in any way should raise the matter directly with the Data Officer or Board of Trustees.

APPENDIX

Personal data document retention periods - policy

Overall guidance

Personal data processed for any purpose must be kept for no longer than is necessary for that purpose.

The appropriate period for retention will be either:

1. The statutory minimum period set out in law
2. Informed by practices advised by professional organisations, or
3. A matter of good business practice, balancing judgement and risk

BF will endeavour to:

- Document and keep under review the length of time we retain personal or special category data
- Consider the purpose/s for which we hold the data in deciding whether (and for how long) to retain them
- Retain personal data only when we can establish a legal basis for processing/storing them
- Maintain a record of our data processing activities, including where possible, the envisaged time limits for erasure of the different categories of data
- Securely delete data that is no longer needed for our identified purposes or for which there is no legal basis for retention
- Update, archive or securely delete data if they go out of date.

Our current document retention schedule is set out below, indicating in each case the basis for our retention period decision.

Some categories of data are not currently processed by BF (eg pension records) but are included in this schedule for future reference to support the development of a long term and comprehensive data protection framework.

Document	Minimum Retention Period	Authority/Justification
BF sessions		
Parent personal data and contact information	3 years from attendance at latest event	Good practice
Child personal data	3 years from attendance at latest event	Good practice
Child health and wellbeing record	To be destroyed immediately after participation at session, with the exception of name and photograph	Name and photograph stored for identification purposes of children on photos in event of SAR
Safeguarding records	Held until the child concerned reaches 25, unless there is either an established statutory need to retain the record, or there is a prospect of the record being required as evidence in legal proceedings	NSPCC guidance Information and Records Management Society (IRMS), 2016. Northern Ireland: the government recommends that child protection files should be kept until the child's 30th birthday (Department of Education, 2016).
Tutor personal and contact data	3 years from latest engagement	Good practice
Tutor engagement contract	3 years from first engagement	Good practice
Tutor and Ambassador DBS / PVG / Access NI, or other equivalent record check	A copy of the actual check will only be kept if there is a dispute about the results of the check – 6 months. Otherwise a confidential record of the following will be kept: • the date the check was completed • the level and type of check (standard/enhanced/barred list check and the relevant workforce) • the reference number of the certificate • the decision made about whether the person was employed (with reasons). - 6 years	NSPCC guidance Limitation Act 1980 – limitation for negligence (made by public etc.)
Teacher Observation DBS/PVG/Access NI, or equivalent record check	A copy of the teacher's check is provided to BF in order to observe young people's online sessions. This will only be kept if there is a dispute about the results of	NSPCC guidance Limitation Act 1980 – limitation for negligence (made by public etc.)

	the check – 6 months. A confidential record of the following will be kept: • the date the check was completed and by whom • the level and type of check (standard/enhanced/barred list check and the relevant workforce) • the reference number of the certificate - 6 years	
Ambassador personal and contact data	3 years from latest engagement	Good practice
Ambassador engagement contract	3 years from first engagement	Good practice
Employee Relations (and trustee relations, where applicable)		
Application forms and interview notes (for unsuccessful candidates – staff employment, volunteers, trustees)	6 months to a year	Recommended practice (CIPD) Defamation Act 1996 1-year limitation (in respect of any shared comments)
Applications (successful – staff employment, volunteers, trustees)	6 months following end of probation period – may retain useful data eg skills	Assess and verify suitability for role Limitation incl. EC for unfair dismissal and discrimination claims etc.
Authorised absence records (annual leave, time off for dependents, jury service etc.)	2 years from when the entry was made	Working Time Regulations 1998 Part II
Contracts, offer letters and variations (including any flexible working outcome)	6 years following end of employment	Limitation Act 1980 – limitation for breach of contract
Criminal record checks and disclosures (eg a DBS certificate)	6 years following end of employment	Limitation Act 1980 – limitation for negligence (made by public etc.)
Capability and disciplinary documents (substantiated)	2 years following the issue of the warning	TUPE 2006 Case law permitting expired warnings to be referred to (but not built upon). Unreasonable to refer back after 2 years
Driving licence (if required)	Duration employee drives on business plus 3 years *consider any insurance obligations	Limitation Act 1980 – 3-year limitation for negligence for a known act/incident
Grievance documents	6 months following end of employment	Limitation incl. EC for 'last straw' constructive dismissal and discrimination claims etc
Maternity medical records	3 years after the end of the tax year in which the	The Statutory Maternity Pay (General) Regulations 1986 as

	maternity period ends	amended
Medical capability documents and records incl. OH reports	6 months following end of employment	Equality Act 2010 Limitation incl. EC for unfair dismissal and discrimination claims etc.
Professional insurance (including insurance for driving on business), licence to practice and professional registrations.	6 years following end of employment *consider any insurance, regulatory or supervision obligations eg GMC, NMC, CQC, FCA	Limitation Act 1980 – limitation for negligence (made by public etc.)
Qualifications	6 years following end of employment	Limitation Act 1980 – limitation for negligence (made by public etc.)
Right to work checks	Two years after employment	Recommended practice (Home Office)
Redundancy – documentation	6 years following end of redundancy	Recommended practice (CIPD) Limitation Act 1980
References received for employment	6 months following end of probation period *consider any insurance, regulatory or supervision obligations eg GMC, NMC, CQC, FCA	Assess and verify suitability for role Limitation incl. EC for unfair dismissal and discrimination claims etc.
References issued for employment	1 year	Defamation Act 1996 1-year limitation (in respect of any shared comments)
Sickness records and unauthorised absence records	6 months following end of employment Use pseudonyms where feasible	Limitation incl. EC for unfair dismissal and discrimination claims etc. Recommended practice (data laws)
Sickness and injury records (work related) (other than those listed under 'Health and Safety')	15 years	3 years for personal injury claim 15 years for negligence (in respect of latent damage) Limitation Act 1980
Subject access request letters	1 year following completion of a request	May charge a fee for repeat copies. May be unreasonable to charge a fee after 12 months.
Whistle-blowing – reports and documents linked to an investigation which is partially or wholly substantiated.	6 months following the outcome of the report or any remedial action taken because of the report	Public Interest Disclosure Act 1998 ('PIDA 1998') Employment Rights Act 1996
Whistle-blowing – documents linked to an entirely unsubstantiated claim	Remove immediately any personal data	Recommended practice (IAPP)
Health and Safety		
Accident books, records and reports	15 years	3 years from last entry (or until person is 21 years old) The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and max. 15 years for negligence (in

		respect of latent damage) Limitation Act 1980
Assessments under health and safety regulations and records of consultations with safety representatives and committees	Indefinitely	Recommended practice (CIPD)
First aid training	6 years after employment	Health and Safety (First-Aid) Regulations 1981
Fire warden training	6 years after employment	Fire Precautions (Workplace) Regulations 1997
H&S representatives training	5 years after employment	Health & Safety (Consultation with employees) Regulations 1996
H&S training - employees	5 years after employment	H&S Information for Employees Regulations 1989
Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)	5 years from the date on which the tests were carried out	The Control of Substances Hazardous to Health Regulations 1999 and 2002
Risk assessments	Indefinite	Recommended practice (CIPD)
Payroll and Finance		
Accounting records	3 years	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
Expenses and petty cash records	6 years following year end	Companies Act 1985, section 222 as modified by the Companies Act 1989 and Companies Act 2006
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended
Inland Revenue/HMRC approvals	Permanently	Recommended practice (CIPD)
National Minimum Wage records	3 years after the end of the pay reference period following the one that the records cover	National Minimum Wage Act 1998
Statutory Maternity Pay records, calculations, certificates (Mat B1s) and leave	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 as amended and Maternity & Parental Leave Regulations 1999
Statutory Paternity Pay records, calculations and leave	3 years after the end of the tax year in which the maternity period ends	Maternity & Parental Leave Regulations 1999
Statutory Shared Parental Pay records, calculations, certificates (Mat B1s), notices and leave	3 years after the end of the tax year in which the maternity period ends	Maternity & Parental Leave Regulations 1999

Wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970.
Benefits		
Pension scheme investment policies	12 years from the ending of any benefit payable under the policy however no information should ever be retained unless it is a necessary consequence of the funding	Recommended practice (ICO)
Pension records	12 years after benefit ceases. Avoid access unless required	Recommended practice (CIPD)
Retirement Benefits Schemes – records of notifiable events	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995
Working time		
Timesheets, overtime records and other documents relating to working time	2 years from date on which they were made	Working Time Regulations 1998 Part II

Record type	Retention period
Concerns about a child/young person	The record will be kept for 25 years after the member has left the organisation, or longer if a complaint has been made in respect of the case or legal proceedings.
Concerns about an adult	The record will be kept until the person reaches the age of 65 or for 10 years, whichever is longer (IRMS 2016)/NSPCC GUIDANCE 2018)