Data Protection Policy

1. Our Aim

(1) Tees Valley Arts needs to keep certain information on its trustees, employees, volunteers and service users to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

(2) Tees Valley Arts is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

(3) The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within Tees Valley Arts.

2. About Our Policy

(1) This policy covers all trustees, employees and volunteers.

(2) In line with Article 5 of the GDPR, Tees Valley Arts will ensure that personal data will be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) 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;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 GDPR in order to safeguard the rights and freedoms of individuals; and
f) 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.

(3) The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

(4) **Types of Information Processed**

The following types of information are processed by trustees, employees and volunteers, as appropriate, by a mixture of paper and computer systems and include:

a) **Trustee Information** such as is necessary for regulatory purposes (basis of processing: public task);

b) **Employee Information** including but not limited to, contact details, bank account details, payroll information, supervision and appraisal notes (basis of processing: contract and public task);

c) **Volunteer Information** including but not limited to, contact details, emergency information, action plans, supervision and feedback notes, and other details which may from time to time be required by specific funders (basis of processing: contract);

d) **Membership Information** such as is necessary for regulatory purposes (basis of processing: public task);

e) **Service User Information** including but not limited to, contact details, emergency information and other details which may from time to time be required by specific funders (basis of processing: contract).

(5) **Notification to the Information Commissioner**

a) The needs we have for processing personal data are recorded on the public register maintained by the Information Commissioner. We notify and renew our notification on an annual basis as the law requires.

b) If there are any interim changes, these will be notified to the Information Commissioner within 28 days.

c) The name of the Data Controller within our organisation as specified in our notification to the Information Commissioner is Tees Valley Arts.

3. Our Responsibilities

(1) The overall responsibility for personal data rests with our governing body, the Board of Trustees.

(2) The Board of Trustees delegates the implementation of this policy to the Executive Director. The Executive Director is responsible for:

- understanding and communicating obligations under the Data Protection Act 2018 and the GDPR
- identifying potential problem areas or risks
- producing clear and effective procedures
- notifying and annually renewing notification to the Information Commissioner
- notifying the Information Commissioner of any relevant interim changes

(3) All trustees, employees and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

(4) Breach of this policy will result in disciplinary proceedings.

4. Our Commitments

(1) To meet our responsibilities trustees, employees and volunteers will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

(2) We will ensure that:

- Everyone managing and handling personal information is trained to do so.
- Anyone wanting to make enquiries about handling personal information, whether a trustee, employee, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.
- Queries about handling personal information will be dealt with swiftly and politely.

(3) We will seek to create an environment in which data protection and security is at embedded into the approach of all trustees, employees and volunteers, as well as by contract suppliers and partners.

(4) To ensure that we are meeting the aims and the spirit of this policy we will:

(a) Discuss and review how well we are implementing this policy, and (adjust our practices/develop an action plan) where necessary;

(b) Assess any significant new or revised policies and procedures for their impact on data protection and security;

(c) Embed data protection and security into our development plans;

(d) Ensure our employment practices and procedures are consistent with the aims of this policy.

(5) **Data Security**

Tees Valley Arts will take all necessary steps to ensure that data, particularly personal data, is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

(a) All files stored electronically on our internal network will only be stored on systems that are encrypted to the XTS-AES 256-bit encryption standard;

(b) All files accessed through our internal network will only be accessible to a user that has been granted appropriate role-based access and is accessing the files through a strong password, using two-factor authentication where possible, and across an encrypted connection;

(c) All files stored on our internal network will be stored on Btrfs formatted file system on a RAID platform which protects them from mechanical hard-drive failure, as well as enabling them to benefit from hourly snapshotting of each file with those snapshots being retained as follows: 12 hourly, 3 daily, 1 weekly, 1 monthly, 1 yearly; enabling immediate restoration of any file when necessary;

(d) All files stored on our internal network are independently backed up both onsite, to allow for quick restoration, as well as offsite to a dedicated unit located in a different building and compliant with (a) to (c). The backup service includes automatic integrity checks, run daily, to ensure that any corruption is quickly identified and notified to the system administrator by email;

(e) All essential files are also backed up in immediately accessible online storage platforms, which means in the advent of catastrophic system failure meaning that so long as internet connection can be secured files can be accessed subject to (b) immediately. Archive files are also backed up to long-term storage in Amazon S3 drive located within the EU;

(f) All internal networks and all devices used to access those networks within the organisation are secured by firewalls and a managed anti-virus service that can be remotely updated and is able to email threat notifications to the designated administrator;

(g) All files stored remotely on an employee's computer or other electronic device are only permitted where that device meets a minimum level of XTS-AES 128-bit encryption standard such as Apple File Vault or Microsoft BitLocker for the drive on which the data is stored, and will only be permitted through an approved file sharing platform such as Microsoft OneDrive that allows the organisation to remotely remove the data from the device;

(h) All devices accessing the internal network will be kept up-to-date with the most recent software and firmware patches provided by the manufacturers and/or vendors and devices will be set to auto-update where available.

(i) The organisation has a Mobile Device Management policy provided by Google for Nonprofits and used to ensure a minimum level of security including: enforcing the device only be accessed through a pin/password protection/fingerprint recognition or facial recognition as necessary; allow the devices to be tracked, remotely wiped or remotely as necessary; keep applications on the device up-to-date;

(j) All passwords used to access services external to the internal network will use in the first instance our Google Apps service as an SSO, which is secured by two-factor authentication, and where this is not possible randomised passwords will be used, generated and stored in a password management application;

(k) Email and software services are provided to the organisation by Google for Nonprofits, which are continuously backed up to our internal server using Active Backup for GSuite;

(l) Software services are provided to the organisation by Microsoft Office 365, which are continuously backed up to our internal server using Active Backup for Office 365;

(m) The organisation does not use USBs to exchange sensitive data;

(n) The organisation will endeavour not to exchange any sensitive data by post and when it is necessary to do so it will always send that data via a tracked, proof of delivery service that requires a signature by the recipient;

(o) All sensitive paper documentation that is stored onsite, will be stored in a lockable cabinet and when it is disposed of will be destroyed by Cleveland Data Shred Ltd and that destruction certificated;

(p) Any external data collected is subject to pseudonymisation and anonymisation where necessary.

If despite the above measures there is a data breach that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data then we will investigate that breach and assess whether or not it poses a risk to people and if there is a likely risk we will report that data breach to the Information Commissioner's Officer within 72 hours of the breach being identified. All breaches – even if they do not constitute a risk to people – will be reported internally to the Chair and Vice Chair of the Board.

These data security provisions meet the standard of the guidance provided by the National Security Centre in their Cyber Security Small Business Guide and will be revised and updated as this guidance changes.

(6) **Any unauthorised disclosure of personal data to a third party by:**

(a) a trustee may result in personal liability for any penalty arising from a breach that they have made
(b) an employee may result in disciplinary proceedings
(c) a volunteer may result in the termination of any volunteering agreement.

(7) **Subject Access Requests**

(a) Anyone whose personal information we process has the right to know:

- What information we hold and process on them (see c)
- How to gain access to this information (see c)
- How to keep it up to date (see b)
- How long we retain their data (see our Data Retention Policy)
- How to ask to be "forgotten" (see b)
- What we are doing to comply with the Data Protection Act 2018 and the GDPR

(b) They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

(c) Individuals have a right to access certain personal data being kept about them on computer and certain files. Any person wishing to do that should apply in writing to: privacy@teesvalleyarts.org.uk.

(d) We will require proof of identity before disclosing any information.

(e) Queries about handling personal information will be dealt with swiftly, politely and we will ensure that any information is provided within one month, from receiving the written request. If due to the nature and/or complexity of the request we require more time to fulfil it, we reserve the right to extend this response time for up to a further two months and will write to you outlining the reasons why before the end of the initial month.

5. **Working with contractors, suppliers and partners**

(1) It is important to us that suppliers, contractors and any other individual or organisation working on behalf of Tees Valley Arts are aware of and agree to comply with our data protection policy while that work is underway.

6. **Complaints**

(1) If, at any point, you are unhappy with the way in which we have fulfilled our duties commitments in this policy (as outlined in item 4) you can make a complaint through our complaints process, which can be viewed here: https://www.teesvalleyarts.org.uk/resources/policies/complaints/ or if you are not satisfied with our response you are legally entitled to make a complaint to the Office of the Information Commissioner here: https://ico.org.uk/make-a-complaint/.

7. **Review and Action**

(1) We recognise that it is important for us to regularly review this policy to ensure that it reflects up to data protection legislation and best practice.

(2) A review of our Data Protection Policy will be carried out on an annual basis prior to as a minimum and any necessary actions taken.

Adopted: 20 July 2017
Last Revised: 17 January 2019

Source: Based on the GRCC Performance Improvement For All Project (PIFA) Template: http://www.grcc.org.uk/downloads/organisational-support-and-funding-advice/templates/grcc-data-protection-policy-template---amended-for-gem-project-february-2017.doc