Data Protection Policy

This Data Protection Policy has been produced to ensure compliance with the Data Protection Act 2018 (DPA), General Data Protection Regulations (GDPR) and associated legislation, and it incorporates guidance from the Information Commissioner's Office (ICO). The DPA gives individuals rights over their personal data and protects individuals from the erroneous use of their personal data. This Policy has been produced to ensure its compliance with the DPA 2018, incorporates guidance from the ICO, and outlines the Companies' overall approach to its responsibilities and individuals' rights under the DPA 2018.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

This Policy applies to all workers and employees, partners and third parties and others who may process personal information on behalf of the STEAM Ahead CIC. The Policy also covers any staff and third parties who may be involved in research or other activity that requires them to process or have access to personal data, for instance as part of a research project or as part of professional practice activities. If this occurs, it is the responsibility of the relevant third-party organisations to ensure the data is processed in accordance with the DPA 1998 and that their staff are advised about their responsibilities.

The member(s) of staff responsible for data protection is Aaron Bourne, Director.

Data Covered by this Policy

Personal data is information relating to an individual where the structure of the data allows the information to be accessed i.e. as part of a relevant filing system. This includes data held manually and electronically and data compiled, stored or otherwise processed by STEAM Ahead CIC, or by a third party on its behalf.

Sensitive personal data is personal data consisting of information relating to:

- Racial or ethnic origin
- Political opinions, Religious beliefs or other beliefs of a similar nature
- Membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

The DPA 2018 requires the School, its staff and others who process or use any personal information must comply with the eight **data protection principles**. The principles require that personal data shall:

1. Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
3. Be adequate, relevant and not excessive for those purposes
4. Be accurate and kept up to date

5. Not be kept for longer than is necessary for those purpose
6. Be processed in accordance with the data subject's rights
7. Be kept safe from unauthorised or unlawful processing and against accidental loss, destruction or damage
8. Not be transferred to a country or territory outside the European Economic Area (unless that country has equivalent levels of protection for personal data)

Responsibilities

The **Data Protection Officer** (DPO) for STEAM Ahead CIC is the Operations Director. This role handles the day-to-day issues which arise, and to provide staff of the Company with guidance on Data Protection issues to ensure they are aware of their obligations. The DPO has the following responsibilities:

- The DPO is responsible for the management of records at the school. The DPO is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy and are disposed of safely and correctly.
- The DPO is responsible for promoting compliance with this policy and reviewing the policy on an annual basis, in conjunction with the Board of Directors.

Workers and employees of the STEAM Ahead CIC are expected to:

- Familiarise themselves and comply with the eight data protection principles
- Ensure any possession of personal data is accurate and up to date
- Ensure their own personal information is accurate and up to date
- Keep personal data for no longer than is necessary
- Ensure that any personal data they process is secure and in compliance with related policies and strategies
- Acknowledge data subjects' rights (e.g. right of access to *all* their personal data held by STEAM Ahead CIC) under the DPA 2018, and comply with access to records
- Ensure personal data is only used for those specified purposes and is not unlawfully used for any other business
- Obtain consent with collecting, sharing or disclosing personal data
- Contact the DPO for any concerns or doubt relating to data protection to avoid any infringements of the DPA 2018.

All new members of staff will be required to complete a mandatory information governance module as part of their induction and existing staff will be requested to undertake refresher training on a regular basis.

STEM Partners and third parties involved in research are expected to:

- Comply with the six data protection principles
- Comply with any security procedures implemented by the STEAM Ahead CIC.

All staff will be provided with and have the expectation to comply with an '**Acceptable Use of ICT Code of Practice**' that is part on the Staff Handbook, induction training and is display in staff areas. These expectation are given in Appendix 1.

Obtaining, Disclosing and Sharing Staff Records

- Only personal data that is necessary for a specific Company related business reason should be obtained.
- Staff are informed about how their data will be processed when they agree to the Data Processing Consent Notice upon induction.
- Upon acceptance of employment by STEAM Ahead CIC, members of staff also consent to the processing and storage of their data.
- Data must be collected and stored in a secure manner.
- Personal information must not be disclosed to a third party organisation without prior consent of the individual concerned. This also includes information that would confirm whether or not an individual is or has been an applicant, worker or employee of the Company.
- STEAM Ahead CIC may have a duty to disclose personal information in order to comply with legal or statutory obligation. (*The DPA 2018 allows the disclosure of personal data to authorised bodies, such as the police and other organisations that have a crime prevention or law enforcement function. Any requests to disclose personal data for reasons relating to national security, crime and taxation should be directed to the DPO*).
- Personal information that is shared with third parties on a more regular basis shall be carried out under written agreement to stipulate the purview and boundaries of sharing. For circumstances where personal information would need to be shared in the case of ad hoc arrangements, sharing shall be undertaken in compliance with the DPA 2018.

Under the DPA 2018, individuals (both staff and students) have the right of access to their personal data held by the Company. This applies to data held in both paper and electronic format, and within a relevant filing system. Any individual who wishes to exercise this right should make the request through submitting a Subject Access Request Form. This is available by contacting the DPO.

The Company may not charge fee. It will only release any information upon receipt of the completed Subject Access Request Form, along with proof of identity or proof of authorisation where requests are made on the behalf of a data subject by a third party. The requested information will be provided within the statutory timescale of 1 month from receipt of the completed form.

Staff personal files will include:

- Forename (others), Surname (plus previous), gender, date of birth, National Insurance Number, DfE Number (if appropriate), ethnic origin, details of SEND (if appropriate), allergies/medical conditions, current/previous (5 years) addresses, contact details, academic record, previous employment record, previous convictions, banking details and names/contacts for two referees (including referee statements) – this information will be held for the term of employment plus 6 years.
- Timesheets, expenses/mileage claims (including payment details) – held for the term of employment plus 6 years.
- Pay, NI, pension details - held for the term of employment plus 6 years.

- Annual, interim, monitoring performance appraisal information – held for current year plus 5 years.
- Training record - held for the term of employment plus 5 years.
- Enhanced DBS Certificate - held for the term of employment (annual update) – worker/employee keeps certificate; copy placed on file.
- Association certification (e.g. driver, H&S, safeguarding, etc) - worker/employee keeps certificate; copy placed on file.
- Evidence of right to work in the UK (if appropriate) - held for the term of employment plus 2 years.
- Internal promotion record (including applications, interview records and line-manager references) - held for the term of employment plus 5 years.
- Disciplinary record - oral warning (date of warning plus 6 months); written warning (date of warning plus 12 months); dismissal with notice (until third-stage meeting); dismissal (date of issue plus 6 years); all investigation information (held during and for the term of employment plus 5 years unless unfounded); probationary information (held for the term of employment plus 5 years).
- Grievance and incident record - held for the term of employment plus 6 years.
- Allegation information about safeguarding/child protection – destroyed if unfounded; 25 years after the pupil's date of birth if proven.
- Director written reference (if requested) for job applications – updated as necessary; held for the term of employment.

Obtaining, Disclosing and Sharing Customer Records

A customer data for STEAM Ahead CIC is specifically data on children and their parents/guardian that is provided upon on-line or paper application to an activity, performance data linked to a specific child collected during the course of an activity or information relating to injury or complaints. All application data provided on paper will be transferred to electronic format as soon as is possible prior to activity commencement and then will be disposed of securely (exceptions listed below).

Customer records will include the following information and will be held either electronically or in paper form as part of a specific activity data set. This data is held centrally on a secure file that can be accessed by Directors, administration staff and other staff that are authorised to do so (e.g. STEM Managers). The associated electronic file can be accessed remotely by specific password-protected Company laptops/tablets during the course of an activity. Authorised staff may also hold paper data (e.g. consent forms) during the course of an activity.

- Child Forename, Surname, gender, date of birth, current school, current school year group, ethnic origin, detail of SEND (if appropriate) and details of any allergies or other medical conditions that are important to be aware of.
- Pupil images used for identification purposes.
- Emergency contact details and the name of the pupil's doctor.
- Names of parents/guardians, including their home address(es) and telephone number(s).
- Scanned and paper parental/guardian consent forms for STEM visits (where no major incident occurred).
- Child performance and survey data collected during an activity (see STEM Data Collection & Dissemination Policy).

During the activity, all involved staff will have access to child forename and surname, parental/guardian names, emergency contact numbers, allergy/medical information (if appropriate) and consent information on all children involved. This is for attendance and safeguarding reasons. Child performance and survey data will be collected in both electronic and paper format and will be used and shared widely with the children during an activity. Following the activity, the above customer records will be held for 1 month to allow for anonymous data analysis and then will be securely disposed of.

Customer data collected prior to, during or immediately following an activity that will be held securely as hard copies (locked filing cabinet) for longer than 1 month includes:

- Consent forms for the use of pupil images for display and marketing purposes – in-line with the agreed consent period.
- Consent forms for STEM visits where a major incident occurred - 25 years after the pupil's date of birth on the pupil's record (permission slips of all pupils on the trip will also be held to show that the rules had been followed for all pupils)
- Correspondence with parents about minor issues, e.g. behaviour – 5 years following the activity.
- Records of complaints made by parents or children – during the investigation; 5 years following decision.
- Accident and incident information – for minor incidents 5 years after activity; for major incidents 25 years after the pupil's date of birth.
- Pupil information and investigation data that relates to any safeguarding/child protection allegations about staff – held during the course of investigation; securely destroyed immediately if unfounded; 25 years after the pupil's date of birth if proven.
- Pupil information if there is ongoing legal action.

Customer data will also include contact details and engagement records/logs for schools and partners involved in the development and delivery of Company associated activities.

Retention, Security and Disposal

- Recipients responsible for the processing and management of personal data need to ensure that the data is accurate and up-to-date. If a worker, employee or applicant is dissatisfied with the accuracy of their personal data, then they must inform the DPO.
- Personal information held in paper and electronic format shall not be retained for longer than is necessary. In accordance with principle 2 and principle 4 of the DPA 2018, personal information shall be collected and retained only for business, regulatory or legal purposes.
- In accordance with the provisions of the DPA 2018, all staff whose work involves processing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage and ensure appropriate measures are in place to prevent accidental loss or destruction of, or damage to, personal data.
- Staff working from home will be responsible for ensuring that personal data is stored securely and is not accessible to others.
- All staff should ensure that data is destroyed in accordance with the Retention Schedule when it is no longer required.

- Personal data in paper format must be shredded or placed in the confidential waste bins provided. Personal data in electronic format should be deleted, and CDs and pen drives that hold personal data passed to the DPO for safe disposal. Hardware should be appropriately degaussed so that it conforms to DPA and GDPR requirements.

Transferring Personal Data

- Any transfer of personal data must be done securely. Email communication is not always secure and sending personal data via external email should be avoided unless it is encrypted with a password provided to the recipient by separate means such as via telephone.
- Care should be taken to ensure emails containing personal data are not send to unintended recipients. It is important that emails are addressed correctly and care is taken when using reply all or forwarding or copying others in to emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.
- Personal email accounts should not be used to send or receive personal data for work purpose.

Staff will be given their own user ID and password for use on the Company network. These must be kept secure and not shared. The Company disclaimer that automatically appears at the end of emails notifies the recipient that any correspondence may be monitored. This disclaimer must not be removed.

Reporting a Data Security Breach

STEAM Ahead CIC are required under DPA and GDPR to ensure that every care is taken to ensure to protection of personal data from incidents (either deliberate or accidental) to avoid a data protection breach that could compromise security. We have in place a framework designed to ensure security of all personal data during its lifecycle, including clear lines of responsibility.

It is important the Company responds to a data security breach quickly and effectively. A breach may arise from a theft, a deliberate attack on Company systems, unauthorised use of personal data, accidental loss or equipment failure. Any data breach should be reported to the DPO immediately (or as soon as is practical (the Company has only 72 hours to report a breach to the Information Commissioner) and should include:

- Full and accurate details on the incident. Nature of the incident and (if appropriate) the people involved.
- Dates and times.

Any breach will be investigated and will treat any breach as a serious issue. Each incident will be investigated and judged on its individual circumstances and addressed accordingly. A full investigation will be undertaken within 24 hours of the breach being discovered/reported (immediate containment if it is currently happening). The DPO will seek advice as to notification of individuals and other organisations.

Data security is an on-going priority of STEAM Ahead CIC and, as such, we will always strive to improve procedures and quickly review incidents to minimise future risks.

Information Available under the Freedom of Information Act 2000

Data Protection Policy

The classes of information that we undertake to make available freely are organised into five broad topic areas:

- **Company contact details** on website and marketing information. This includes customer electronic booking and communication.
- **Activity prospectus and calendar of events** on website and marketing information. This includes all information to support parents, guardians, children, partners and other organisations to be fully aware of the aims, nature and scope of Company activity in order to make informed choices about involvement.
- Some STEM partners and funders will be offered a shortened version of the **Company 3-year business plan**.
- **Key policy documents** available for view on the website. These are available in a format that supports understanding and potential action. Documents will include: Equal Employment Opportunities Policy, Staff Recruitment Policy, Customer Complaints Policy, Safeguarding and Child Protection Policy and the STEM Data Collection & Dissemination Policy.
- STEM Camp and other activity promotion will include **case study and on-going activity reflections** on website and social media. These will include child/parent/partner quoted reflections and photographs/videos of children engaged in activity. All permissions will be sought and kept on-file until the item is removed from public view. This may include anonymised headline data on STEM performance and aspiration.

Information that we will make available in paper form by direct request through our website include:

- Additional policy documents
- Anonymised data related to general and group performance and STEM aspiration for children who have engaged in activities (this information will be shared with STEM partners at annual performance meetings and will be written for this audience).

All current staff will have a copy of staff handbooks that includes all necessary procedural and policy information to carry out specific roles. Staff should not share any of this information to third parties and may also request other Company documentation as necessary.

No information that can identify individuals concerning staff or customers will be shared with the general public unless consent is requested and provided.

This policy has due regard to legislation & guidance including General Data Protection Regulation (GDPR), Freedom of Information Act 2000, Limitation Act 1980 (as amended by the Limitation Amendment Act 1980), Data Protection Act 2018, Information Records Management Society (2016) 'Information Management Toolkit for Schools' and DfE (2018) 'Data protection: a toolkit for schools'

Data Protection Policy

Acceptable Use of ICT Code of Practice

- In using ICT, you must follow the Company aims, ethos and **consider the work and feelings of others**.
- You must not use the system in a way that might cause annoyance or loss of service to other users.
- You must not bring the Company into disrepute by the use of electronic communication.
- **You must keep your user ID and password secure**. You must not share it with others, or allow another person to use your account. You are responsible for all activity on the devise whilst you are logged on, even if it is not you that has done so. Do not log on to more than one devise at a time.
- **You must log off from the device you are using** at the end of your session and wait for the standard login screen to reappear before leaving.
- **You must not misuse the system** to use facilities or gain access to files you are not allowed to use.
- You must not attempt to install / re-configure software to explore or harm the system.
- Do not connect to hardware that may be detrimental to the system.
- **If you suspect that your device has a virus**, you must report it immediately. You should avoid spam.
- **You must manage your own file space** by deleting old data rigorously and by deleting emails you no longer require. It is your responsibility to back-up copies of your work.
- Follow the Data Protection Policy to ensure you are data compliant and prevent a data breach.
- You may import export files using removable devises, but ensure the owner of the material allows you to do so. **You must not plagiarise or copy any material which does not belong to you**.
- Do not copy, download, or plagiarise material on the internet unless the owner of the website expressly permits you to do so.
- **The internet must not be used for private, leisure or inappropriate purposes**. You must not access any newsgroups, links, list-servers, web pages or other areas of cyberspace that could be offensive (e.g. pornographic, racist, illegal) or unsuitable for viewing by children ('inappropriate') at any time during Company business or on Company equipment. You are responsible for rejecting any links to such material.
- **You must not share any attributable information** concerning the Company, staff, children, parents, STEM partners or other linked third parties without consent. You should take care who you correspond with.
- Do not send bank account information and passwords by email unless you trust the other party not to share this information inappropriately.

Please remember, to keep our systems safe and secure and remember that when communicating electronically, you are representing the Company