

Data Protection (GDPR & FOI) Policy

Introduction

This document is a statement of the rationale, aims, principles, approaches, roles, responsibilities and systems, processes and procedures implemented by Steamworks Learning to ensure the safeguarding of personal data (including images) and freedom of information. Guidance and resources provided by the Information Commissioner's Office (ICO) (<https://ico.org.uk/>), the UK Government (<https://www.gov.uk/data-protection>) and the National Society for Prevention of Cruelty to Children (NSPCC) (<https://learning.nspcc.org.uk/online-safety/photographing-filming-children>) have provided the framework for the development of this policy.

The legal framework for this policy is:

- Data Protection Act (1998)
- Freedom of Information Act (FOI) (2000)
- General Data Protection Regulations (GDPR) (2018)

Although, as a not-for-profit organisation, STEAM Works Learning is not required to register with the Information Commissioner's Office (ICO), we audit and review our data protection policies and practices in line with the guidance given by the ICO.

Rationale

The Data Protection Act 1998, Freedom of Information Act (2000) and General Data Protection Regulations (2018) establish a framework of rights and duties which are designed to safeguard personal data (including images) and the rights of individuals to access data about them. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

As Steamworks Learning collects and uses information about its staff, volunteers, children and young people who come into contact with the organisation (data subjects) in order to carry out its work, this information must be collected and dealt with appropriately – whether on paper, electronically, or recorded on other material – and safeguards implemented to ensure compliance with current UK legislation and regulations.

Aims and Principles

Steamworks Learning regards the lawful treatment of personal information (including images) as imperative and therefore ensures that all personal information (including images) is treated lawfully and in accordance with current UK regulations by:

- adhering to the Principles of Data Protection, as detailed in the Data Protection Act 1998, Freedom of Information Act (2000) and General Data Protection Regulations (2018);

- ensuring that all staff and volunteers involved with the collection, processing and disclosure of personal data will be aware of Steamworks Learning's legal responsibilities;
- providing training as and when it is considered appropriate;
- being transparent about how Steamworks Learning uses personal data (including images);
- ensuring that policies are clear and easy for members of the public to access.

The Principles of the Data Protection Act (1998)

(<https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>)

The data protection principles are summarised as:

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 is met and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met;
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- Personal data shall be accurate and, where necessary, kept up to date;
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;
- Personal data shall be processed in accordance with the rights of data subjects under this Act;
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Principles of the Freedom of Information Act (FOI) (2000)

- everybody has a right to access official information. Disclosure of information should be the default – in other words, information should be kept private only when there is a good reason, and it is permitted by the Act;
- an applicant (requester) does not need to give you a reason for wanting the information. On the contrary, you must justify refusing them information;
- you must treat all requests for information equally, except under some circumstances relating to vexatious requests and personal data. The information someone can get under the Act should not be affected by who they are. You should treat all requesters equally, whether they are journalists, local residents, public authority employees, or foreign researchers;
- by treating all requesters equally, you should only disclose information under the Act if you would disclose it to anyone else who asked. In other words, you should consider any information you release under the Act as if it were being released to the world at large.

The Principles of the General Data Protection Regulations (GDPR) (2018)

<https://www.legislation.gov.uk/ukpga/2018/12/contents>

GDPR is concerned with personal data in a form which would allow the individual to be identified. It is not concerned with properly anonymised data about an individual, nor is not concerned with aggregated data about a group.

In accordance with Article 5 GDPR, personal data must be :

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purpose; 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;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- 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;
- 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.

“Personal Data” (including images)

Personal data (including images) is defined in the UK GDPR (2018) as: “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

[\(https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/\)](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/)

Therefore, information about companies and public authorities does not constitute personal data and personal data which is truly anonymised or relates to a deceased person is not subject to UK GDPR (2018). However, although pseudonymised data reduces risks to privacy, this is still personal data and information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual, constitute personal data is therefore subject to UK GDPR (2018).

The GDPR (2018) refers to sensitive personal data (race, ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, genetic/biometric data, health data, sex life/orientation, criminal convictions/offences) as “special categories of personal data” requiring a higher level of protection.

For some children/young people it is necessary for Steamworks Learning to process sensitive data such as the health data of children (medical/SEND needs) to protect the health and wellbeing of the children and young people and meet their individual needs in terms of inclusion, equality and accessibility. (See Inclusion, Equality and Accessibility Policy).

“Data Subjects”

“Data subjects” are the identified or identifiable living individuals to whom personal data relates. Steamworks Learning processes personal data relating to, but not necessarily limited to, employees, volunteers, schools, parents and children and respects the rights of data subjects. Parental consent is required for processing data of children/young people, which the UK government has determined to be under the age of 13 years.

<https://www.legislation.gov.uk/ukpga/2018/12/section/3/enacted?view=interweave>

“Data Controller”

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. A controller can be a company or other legal entity (such as an incorporated partnership, incorporated association or public authority), or an individual (such as a sole trader, partner in an unincorporated partnership, or self-employed professional, eg a barrister). As the Data Controller exercises overall control of the personal data being processed, they are ultimately in charge of and responsible for implementing appropriate technical and organisational measures to ensure processing is carried out in line with the UK GDPR (2018). Steamworks Learning is the Data Controller under the Act and will determine what purposes the information held will be used for and compliance with UK GDPR (2018) and, if required, responsible for notifying the Information Commissioner of the data we hold or are likely to hold, and the general purposes that this data will be used for.

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-are-controllers-and-processors/>

“Data Processor”

A data processor is a person, company, or other body which processes personal data on the data on behalf of the Data Controller. Processors act on behalf of the relevant controller and under their authority, serving the controller’s interests rather than their own. A processor can be a company or other legal entity (such as an incorporated partnership, incorporated association or public authority), or an individual, for example a consultant.

Although a processor may make its own day-to-day operational decisions, they only process personal data in line with a controller's instructions, unless it is required to do otherwise by law. If a processor acts without the controller's instructions in such a way that it determines the purpose and means of processing, including to comply with a statutory obligation, it will be a controller in respect of that processing and will have the same liability as a controller. Employees of the controller are not processors.

Employees of Steamworks Learning operating within the scope of their duties as an employee are acting as an agent of the controller and are therefore part of the controller because they are not a separate party contracted to process data on the controller's behalf.

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-are-controllers-and-processors/>

“Data Protection Officer” (DPO)

Under the GDPR, some organisations need to appoint a Data Protection Officer (DPO) who is responsible for informing them of and advising them about their data protection obligations and monitoring their compliance with them. A data protection officer is a role within a company or organisation whose responsibility is to ensure that the company or organisation is correctly protecting individuals' personal data according to current legislation. Although Steamworks Learning does not need to officially appoint a Data Protection Officer, the director/s are responsible for data protection.

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-officers/>

“Data Processing”

“Processing”, means taking any action with an individual's personal data. This begins when a data controller starts making a record of information about someone and continues until the information is no longer needed and is securely destroyed. If an individual's personal data is stored, it counts as processing even if nothing else is done with it. Other types of data processing include actions such as organising and restructuring the way you save the data, making changes to it, for example, updating an individual's address or record, and sharing it or passing it on to others.

The GDPR (2018) applies to the processing of personal data wholly or partly by automated means and/or to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. The Personal Information collected, processed and stored by Steamworks Learning is set out in the Employee Data Flow Chart (Appendix 1), Privacy Notice for staff (Appendix 2), Booking data flow chart (Appendix 3) and Privacy Notice for parents (Appendix 4).

<https://www.legislation.gov.uk/ukpga/2018/12/section/3/enacted?view=interweave>

Principles into Practice

Steamworks Learning (Data Controller) legitimately collects, processes and stores personal data about employees, volunteers, children/young people and their parents/carers (principal groups) to fulfil its role as an employer and to facilitate the booking of out of school hours workshops and clubs (FabLab). (Appendix 1-4).

Steamworks Learning issues a Privacy Notice to all parents/carers and employees to ensure transparency in the way personal data is collected, stored and processed and provide the reasons it is required and how it is used or shared. Parents/carers use Microsoft Forms to book children/young people on to out of school hours workshops and clubs (FabLab) which meets the requirements of the General Data Protection Regulation (GDPR).

Therefore, in compliance with the principles of the Data Protection Act (1998), Freedom of Information Act (2000) and GDPR (2018) Steamworks Learning will:

- have legitimate grounds for collecting and using personal data for specified/lawful purposes;
- process personal data fairly and lawfully;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and ensure that data is not handled unlawfully;
- comply with what the Act says about notifying the Information Commissioner;
- hold only personal data about an individual that is relevant and sufficient for the purpose it is being held for in relation to that individual;
- take reasonable steps to ensure the accuracy of any personal data obtained and keep up to date as necessary;
- ensure that the source of any personal data is clear;
- carefully consider any challenges to the accuracy of information;
- consider the purpose or purposes the information is held for in deciding whether (and for how long) to retain it;
- archive or securely delete information that is no longer needed or goes out of date;
- uphold the right of individuals to access a their personal data;
- uphold the right of individuals to object to processing that is likely to cause/is causing damage or distress;
- uphold the right of individuals to prevent processing for direct marketing;
- uphold the right of individuals to object to decisions being taken by automated means;
- uphold the right of individuals in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed;
- uphold the right of individuals to claim compensation for damages caused by a breach of the Act.
- have appropriate security to prevent the personal data they hold being accidentally or deliberately compromised;
- design and organise security to fit the nature of the personal data they hold and the harm that may result from a security breach;
- be clear about who is responsible for ensuring information security.
- be ready to respond to any breach of security swiftly and effectively.

Data Privacy Statements

Steamworks Learning maintains an up-to-date “data privacy statement” for each of its principal groups of data subjects (employees, parents/carers). Data privacy statements are available separately and are freely available to data subjects on request. They provide the following specific information for the relevant group of data subjects:

- What personal data Steamworks Learning holds
- How the personal data is kept safe
- What the data is used for
- The “lawful basis” (legal right) of Sheffield Christian Life Centre to hold and process the data
- Who can see the data
- How long the data will be kept
- The data subjects’ rights

Data subjects’ rights

Steamworks Learning is committed to upholding the rights of data subjects, particularly:

- Right to know what data is held
- Right to have a copy of the data held
- Right to object to the “lawful basis” for holding data
- Right to object to the misuse of data
- Right to have data corrected
- Right to be forgotten (to have data removed)

Subject Access Requests (SAR)

All Data Subjects have the right to make a “subject access request” to Steamworks Learning to ask if their personal data is being held or for copies of their personal data. (Appendix 5). If Steamworks Learning receives a “Subject Access Request”, the following actions will be taken within one (calendar) month:

- Confirm whether any personal data about the data subject is being held;
- Provide them with a copy of their personal data, and respecting their “Right of Portability”, if requested, in a “commonly used electronic form” (eg., MS Word, PDF, etc);
- Provide any supporting explanatory materials (e.g. a Data Privacy Statement);
- Steamworks Learning reserves the right to charge a reasonable fee where requests are “manifestly unfounded or excessive” and particularly if they are repetitive. No fee will normally be charged for the first SAR, or where previous SARs have found errors in their data. Where requests are “manifestly unfounded or excessive” and/or repetitive a typical fee will be £20. Steamworks Learning reserve the right to increase this for further SARs to reflect the time taken in processing a SAR.

- If a SAR reveals that any details we held are incorrect, they will be amended without charge.
- Sheffield Christian Life Centre will also take reasonable steps to ensure that this information is kept up-to-date by asking data subjects whether there have been any changes. The Data Protection Act (1998), Freedom of Information Act (2000) and GDPR (2018) extends to all data subjects a right of access to their own personal data. In order to ensure that individuals receive only information about themselves, a formal system for handling requests is in place (See Appendix i). Where a subject access request is received from a data subject, in writing, it is the responsibility of the nominated officer to process these requests.

<https://ico.org.uk/for-the-public/getting-copies-of-your-information-subject-access-request/>

Data Integrity and Security

Steamworks Learning undertakes to ensure that all personal data relating to its principal groups will be stored securely and will only be accessible to authorised personnel who need access to the data to carry out their work and who understand their responsibility to keep personal data secure.

Personal data will be held in as few places as necessary, unnecessary data sets will not be created, and be disposed of appropriately and securely. Steamworks Learning takes responsibility for ensuring that all personal and company data is non-recoverable from any computer system previously used within the organisation which has been passed on/sold to a third party.

When data is **stored on paper**:

- Personal data will be kept in a secure, locked place where unauthorised personnel cannot access it. This also applies to electronic data which has been printed.
- Print-outs of personal data will be kept to a minimum and shredded when no longer required.

When data is **stored electronically**:

- All devices (PCs, laptops, cameras, DVDs, pen-drives, etc) will be protected from unauthorised access, accidental deletion and malicious hacking attempts by using strong passwords that are changed regularly and never shared with unauthorised personnel and anti-virus software.
- Personal data, including photographs, will not be stored on personal devices (mobile phones, tablets, etc)
- The screens of computers will always be locked when left unattended;
- Personal data will never be sent via social media as this form of communication is insecure;
- Personal Data will be encrypted before being transferred electronically by email;
- Copies of personal data will not be saved to personal computers.

Photographic Images

- Photographic images/videos will only be stored on designated devices;
- When photographic images/videos are no longer required, they will be permanently deleted;
- Any member of staff taking and using photograph images/videos of young people (under 18 yrs) must obtain written consent from parents or carers;

- Parents/carers must be given the opportunity to withdraw their consent for the publication of photographic images/videos of their children/young people;
- Photographic images/videos must only be used for Steamworks Learning own publications eg., leaflets, flyers, website, facebook page, and must not contain the names of the children/young people or be intentionally sold or passed on to a third party;
- Participants must be made aware that Steamworks Learning is unable to control the use of photographic images/videos once placed in the public domain.
- Wherever possible, staff should avoid including the children's faces in photographic images/videos.

<https://learning.nspcc.org.uk/online-safety/photographing-filming-children>

“Data Breach”

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Steamworks Learning takes all reported “data breaches” very seriously and will take prompt actions to investigate a suspected data breach, to minimise the effect of any breach, and to reduce the chance of it happening again. The actions will be recorded in a Data Breach Register and if a data subject contacts us about a breach involving their data, they will be informed about the actions taken.

If Steamworks Learning becomes aware of any data breach and considers it has been a ‘high risk’ breach (the requirement to inform individuals is higher than for notifying the ICO), Steamworks Learning will:

- report it promptly to the Information Commissioners Office (within 72 hours where feasible);
- take all reasonable steps to contact or inform the data subjects whose data is involved;

Roles and Responsibilities

The Role and Responsibilities of Steamworks Learning (Data Controller) are to:

- comply with the data protection principles listed in Article 5 of the UK GDPR;
- ensure that individuals can exercise their rights regarding their personal data, including the rights of access, rectification, erasure, restriction, data portability, objection and those related to automated decision-making;
- implement appropriate technical and organisational security measures to ensure the security of personal data;
- use a processor that provides sufficient guarantees that they will implement appropriate technical and organisational measures to ensure their processing meets UK GDPR requirements. This means you are responsible for assessing that your processor is competent to process the personal data in

line with the UK GDPR's requirements. This assessment should take into account the nature of the processing and the risks to the data subjects;

- enter into a binding contract or other legal act with your processors, which must contain a number of compulsory provisions as specified in Article 28(3);
- report personal data breaches to the ICO and, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.
- notify data subjects if a data breach is likely to result in a high risk to their rights and freedoms;
- comply with the UK GDPR accountability obligations, such as maintaining records, carrying out data protection impact assessments and appointing a data protection officer;
- comply with the UK GDPR's restrictions on transfers of personal data outside of the UK;
- cooperate with supervisory authorities (such as the ICO) and help them perform their duties.
- pay the ICO a data protection fee unless exempt.

The role and responsibilities of the Director/s are to:

- ensure that the Data Protection (GDPR & FOI) Policy is updated to reflect changes in legislation and implemented across the organisation;
- ensure that all employees understand their rights and responsibilities within respect to current legislation and guidance regarding Data Protection (1998) and Freedom of Information (2000) and GDPR (2018);
- ensure that all employees involved with the collection, processing and disclosure of personal data understand the processes and procedures within this policy;
- provide the required equipment and resources necessary to ensure data integrity and security;
- appoint a nominated Designated Data Protection Officer (Director/s).

The role and responsibilities of the Designated Data Protection Officer (Director/s) are to:

- Ensure that data integrity and security of personal data in accordance with the procedures and practises detailed in this policy;
- Monitor and review the implementation of the procedures and practises detailed in this policy;
- Process subject access requests;
- Report data breaches to the Information Commissioner's Office.

The role and responsibilities of all employees are to:

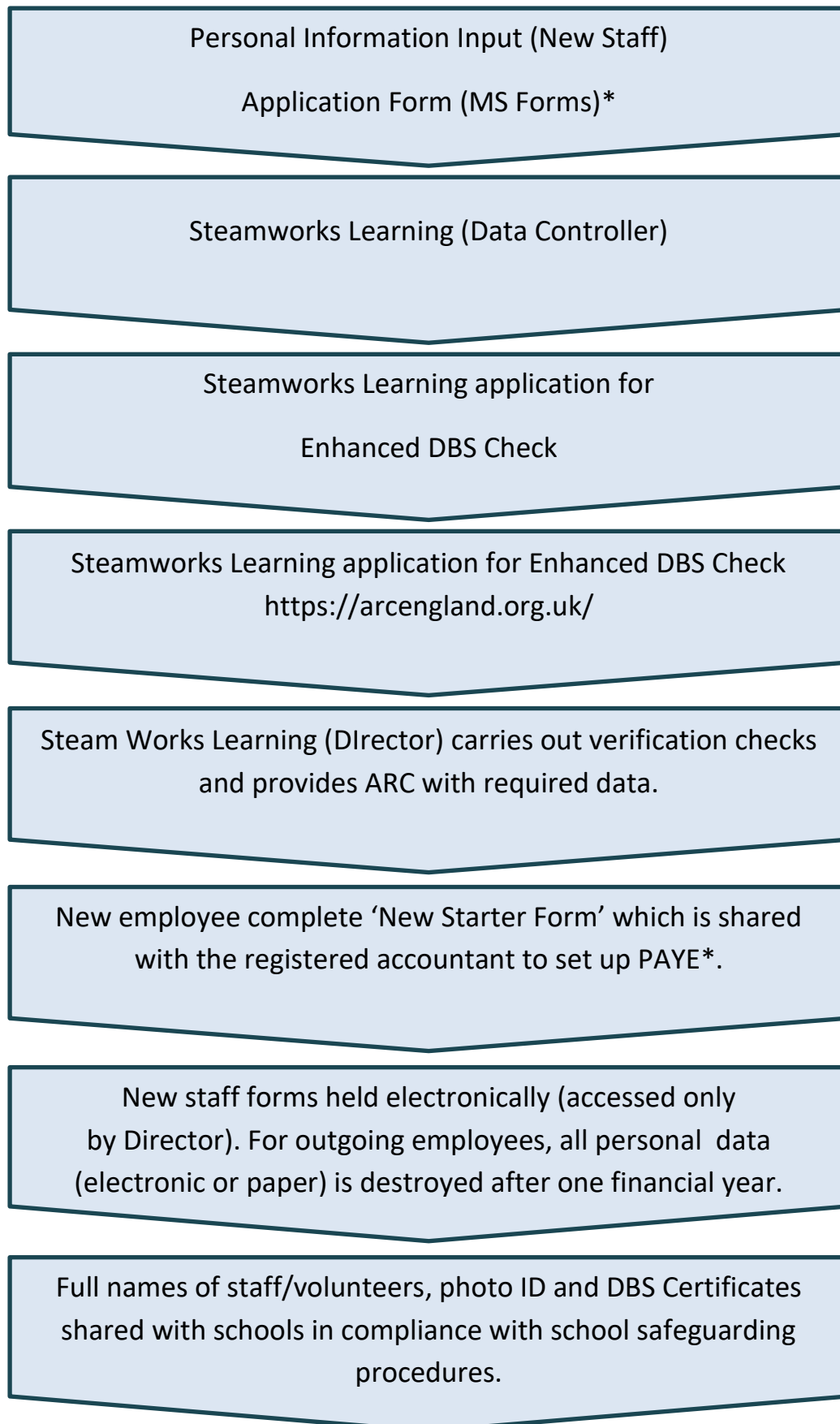
- Adhere to the principles, practices and procedures within this policy and act in accordance with the Data Protection Act (1998) and the Freedom of Information Act (2000) and the GDPR (2018);

Further advice and information is available from the Information Commissioner's Office, www.ico.org.uk or telephone 0303 123 1113.

Approved by: Rosey Andrassy

Date of next review: July 2025

Appendix 1 – Employee Data Flow Chart



*Details Required

Personal Information	Reason Required
Full name of member of staff	Verify ID School safeguarding requirement
Also Known as (other names)	Safer Recruitment requirement
Email address of member of staff	Communicate dates, location, information about work they will carry out and provide updates on policies, procedures, etc
Telephone number of member of staff	Communicate arrangements for work they will carry out Communicate in case of emergencies
Full address and postcode of member of staff	Verify ID Set up PAYE Communicate by post if required
Date of Birth	Verify ID
Driving Licence/Car	Accessibility for clubs
Previous employer/employment	Safer Recruitment requirement
Education	Safer Recruitment requirement
References	Safer Recruitment requirement School safeguarding requirement
NI Number	PAYE Tax Code
Marital Status	PAYE Tax Code
Start date	PAYE Tax Code
Previous Employment/Benefits claimed since 6 th April	PAYE Tax Code
P45	PAYE Tax Code
Annual/weekly basic, gross salary	PAYE Process
Bank Account details and sort code	Transfer of salary/wages directly to member of staff's bank account.

Appendix 2 – Privacy Notice for Employees

Personal Data

Steamworks Learning is a not-for-profit organisation which aims to increase children’s engagement in STEAM (science, technology, engineering, art and maths). When you become an employee at Steamworks Learning, the organisation will keep some data about you. This is “personal data”, because it is about you as a particular person, and it can be linked to you. Steamworks Learning has a legitimate interest in holding data on employees to facilitate PAYE and to carry out DBS checks in accordance with safeguarding requirements and to assess suitability to work with children and young people.

What personal data do we hold?

Steamworks Learning will hold data about you in several ways:

- 1) your **application form** to work for Steamworks Learning - this records your name, address, email address, phone number, if a DBS check was needed, and any unspent criminal convictions.
- 2) your **schedule of work** - this holds data such as your name, address, email address, phone numbers, emergency contact details.
- 3) your **HMRC PAYE records** - these record your name, address, NI number, date of birth, and payments of salary, NI and tax

This is the only data Steamworks Learning will usually hold about you. We do not get data about you in any other way. There may also be information about you in emails. In the event of a grievance, accusation or disciplinary matter, this will be recorded separately.

How do we store your personal data?

All personal data is encrypted and stored electronically on password-protected devices or web-based storage systems (G-drive, MS Cloud, etc) and is accessible only by Steamworks Learning director/s.

What is your data used for?

Your data is only used for purposes directly relating to your employment, particularly:

- 1) To contact you about your employment, if we need to;
- 2) To contact the right person, if you have an accident or are taken ill when at work;
- 3) To make reasonable adjustments if required;
- 4) To maintain PAYE records required by HMRC, and records required by any workplace pension provider.

Does Steamworks Learning have a right to your data?

Under Data Protection legislation, Steamworks Learning needs to have a “lawful basis” for keeping your data, and for using it. There are several types of “lawful basis”. One of them is called “performance of a contract”. When you become an employee, we enter into a “contract” together. You undertake to fulfil your role; we undertake to properly look after you, other people, and our accounts. To do this, we need to hold data about you. That is why the lawful basis for holding your data is “performance of a contract”.

Who can see your data?

The only people who have access to your data is the director/s and Finance personnel. We are as careful as possible to make sure no one else has access to your personal data.

How long do we keep your personal data?

The personal data of employees is held for the duration of their employment and retained for one financial year after the employment has ended. This is so that we can contact you, if we need to ask you any questions about your time as an employee. It also helps us if you ask us for a reference, because you are applying for a job or another volunteer position. All personal data is deleted or shredded securely after this time. Financial records – including PAYE and workplace pension – will be kept for six years after you leave. This is so we can prove that our accounts are correct, and that we have made the right payments. We may keep records of any grievance, dispute or accusation for up to six years.

Who can you speak to if you have a problem or questions?

The Data Protection officer is Rosey Andrassy (rosey@steamworks.org.uk).

Who do we share your data with?

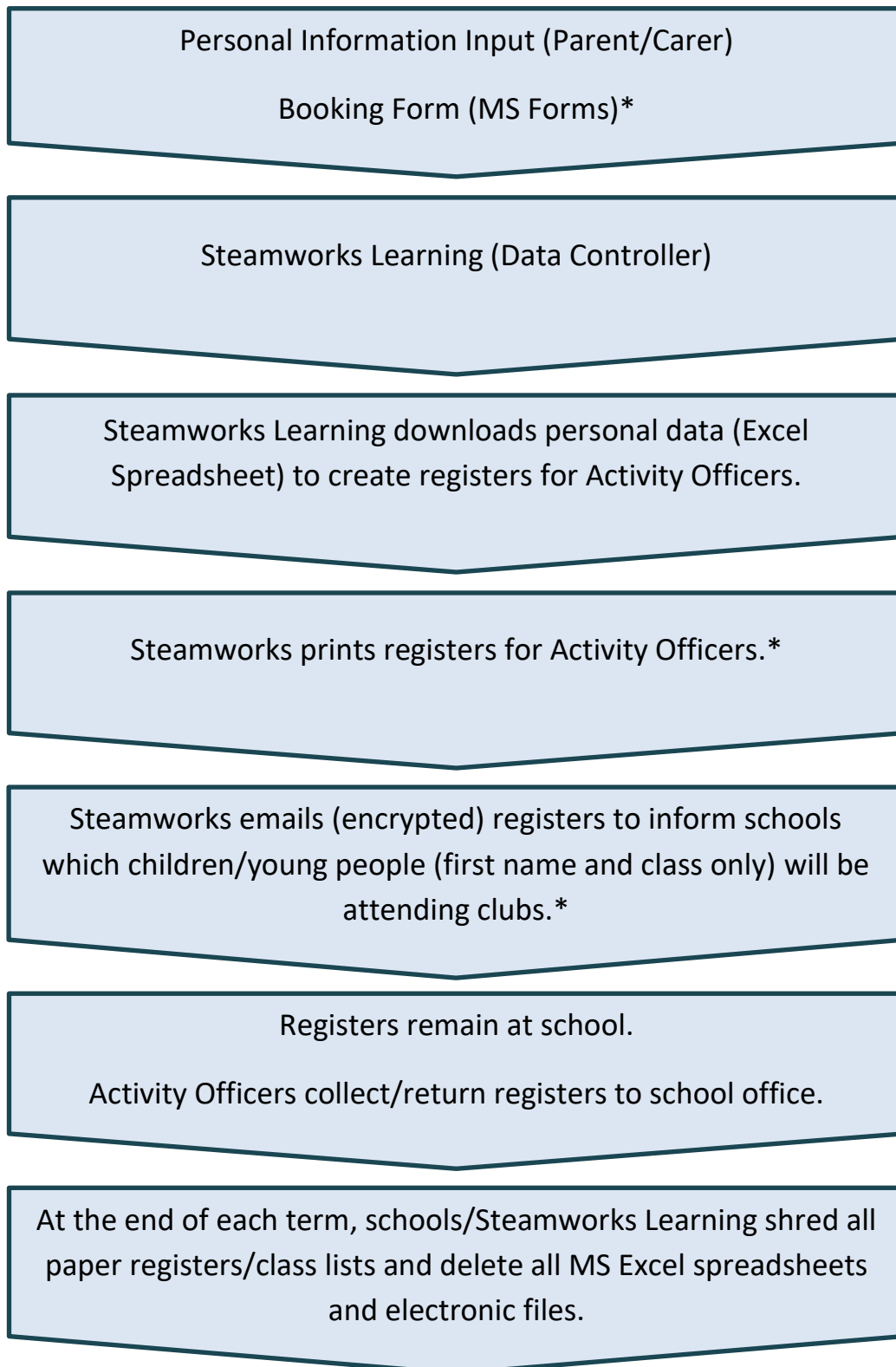
The data in the table (Appendix 1) is shared with the Steamworks Learning accountant and if with ARC ([ARC UK – Association for Real Change](#)) to carry out DBS checks prior to new employees commencing work. We will not share your personal data with third parties for marketing purposes or with any third parties without your consent unless the law requires us to.

What rights do you have?

You have a number of rights under Data Protection legislation:

1. You have a right to know what personal data we hold about you. This Data Privacy Statement describes the data that we will hold. But you can ask if we have any other data about you which is not covered by this Data Privacy Statement.
2. You can ask for a copy of the data we hold about you. This is called a “subject access request”. If you make a “subject access request”, we will give you a copy of all the data we hold about you. We will do this within one month. If it helps, we will give you the data in a computer file.
3. You can object if you think we are using your data in the wrong way. You can also object if you think we don’t have “lawful grounds” for using your data. We will give you a statement explaining why we use your data and explaining the “lawful grounds”. If you are still not happy, you can complain to the Information Commissioner’s Office. If we find we are using your data in the wrong way, we will stop immediately and stop it happening again.
4. If you think there is a mistake in your data, please tell us. You have a right to have it corrected. We may need to check what is the correct data, but will put right any mistakes as soon as possible.
5. Steamworks Learning remove your data after six years. You have a right for this to happen, because we do not need to keep your data any longer than six years.

Appendix 3 – Booking Data Flow Chart



*Details required

Personal Information	Reason Required
Full name of parent/carer	Identification of bookings Match bookings with payments made directly to the bank
Email address of parent/carer	Confirm booking Communicate changes to schedules, times, dates of clubs Communicate information about the content of clubs
Telephone number of parent/carer	Communicate changes to schedules, times, dates of clubs Notify of cancellation of club Discuss payment/booking issues Discuss individual needs (medical, SEN, Disabilities, etc) Contact in case of emergency
Full name of child/young person	Identification within school
Age of child/young person	Check activities are age-appropriate Ensure club booking is correct
Child/young person's class	Communicate with your child/young person's school (numbers, children)
Medical/Health needs	Health & Safety requirement Accessibility, Equality and Inclusion requirement Ensure Activity Officer is aware of individual needs of child/young person (allergies, etc) Make reasonable adjustments to teaching approaches, resources, extra staffing, etc, if possible.
Medication	Health & Safety requirement Ensure Activity Officer is aware of individual needs of child.
SEN and Disabilities	Accessibility, Equality and Inclusion requirement Ensure Activity Officer is aware of individual needs of child/young person (allergies, etc) Make reasonable adjustments to teaching approaches, resources, extra staffing, etc, if possible.
Permission for photographic images/videos	Data Protection (GDPR & FOI) requirement. Safeguarding requirement
Permission to walk home independently	Safeguarding requirement
Gender/ethnicity	Monitoring requirement if funded by the Local authority/Department for Education (DfE)
Emergency contact name and telephone number	Contact in case of emergency if parent/carer uncontactable Health & Safety requirement Safeguarding requirement

Appendix 4 – Privacy Notice for Parents/Carers

Personal Data

Steamworks Learning is a not-for-profit organisation which aims to increase children’s engagement in STEAM (science, technology, engineering, art and maths). When you use the online booking system, Steamworks Learning will keep some data about you and your child/young person. This is “personal data”, because it is about you and your children/young person as a particular person, and it can be linked to you. Steamworks Learning has a legitimate interest in holding data on parents/carers and children/young people to match bookings with payments, communicate information about the club and to fulfil its duties and responsibilities in relation to health and safety, safeguarding and accessibility, equality and inclusion.

What personal data do we hold and what is it used for?

Your personal data is only used for purposes directly relating to the bookings you make for your child/young person and ensure the safety and well-being of your child/young person.

- 1) **Parent/carer name, address, email address, phone number** to confirm/cancel/amend bookings, for communication purposes and in case of emergency;
- 2) your **child’s/young person’s name, age, class** to identify your child within the school, communicate with school and ensure that the club is age-appropriate for your child/young person;
- 3) details about **your child’s/young person’s health and medical needs, including SEN and disabilities** to ensure that Activity Officers are provided with the details they need to keep them safe and, when possible, make reasonable adjustments to meet the needs of your child;
- 4) your **permission for photographic images (including videos) to be taken of your child/young person** to safeguard your child/young person and respect and uphold the rights of data subjects;
- 5) your **permission for your child/young person to make their own way home at the end of the club** to safeguard your child/young person;
- 6) **emergency contact details for a name person/s** to be contacted in case of emergency if you are uncontactable to safeguard your child/young person;
- 7) if the activities are funded by an organisation such as the local council or Department for Education (DfE), details of **your child’s/young person’s ethnicity and gender** may be requested for monitoring purposes – you will be informed when this is the case.

This is the only data Steamworks Learning will usually hold about you. We do not get data about you in any other way but there may be information about you or your child/young person in emails to their school.

How do we store your personal data?

When your personal data is stored electronically, it is encrypted and stored electronically on password-protected devices or web-based storage systems (G-drive, MS Cloud, etc) and is accessible only by Steamworks Learning director/s. When your personal data is stored on paper, it will be stored securely by the school throughout the duration of the booking it relates to.

Does Steamworks Learning have a right to your data?

Under Data Protection legislation, Steamworks Learning needs to have a “lawful basis” for keeping your data, and for using it. There are several types of “lawful basis”. One of them is called “consent”. When you make a booking for your child/young person, you have given clear “consent” for Steamworks Learning to process your personal data for a specific purpose. To do this, we need to hold data about you. That is why the lawful basis for holding your data is “consent”.

Who can see your data?

The only people who have access to your data are the director/s, the Activity Officers and your child/young person’s school. We are as careful as possible to make sure no one else has access to your personal data.

How long do we keep your personal data?

The personal data of parents/carers, children/young people is only held for the duration of the booking. All personal data is deleted or shredded securely after this time.

Who can you speak to if you have a problem or questions?

The Data Protection officer is Rosey Andrassy (rosey@steamworks.org.uk).

Who do we share your data with?

Your personal data is only shared with Activity Officers and your child/young person’s school. We will not share your personal data with third parties for marketing purposes or with any third parties without your consent unless the law requires us to.

What rights do you have?

You have a number of rights under Data Protection legislation:

1. You have a right to know what personal data we hold about you. This Data Privacy Statement describes the data that we will hold. But you can ask if we have any other data about you which is not covered by this Data Privacy Statement.
2. You can ask for a copy of the data we hold about you. This is called a “subject access request”. If you make a “subject access request”, we will give you a copy of all the data we hold about you. We will do this within one month. If it helps, we will give you the data in a computer file.
3. You can object if you think we are using your data in the wrong way. You can also object if you think we don’t have “lawful grounds” for using your data. We will give you a statement explaining why we use your data and explaining the “lawful grounds”. If you are still not happy, you can complain to the Information Commissioner’s Office. If we find we are using your data in the wrong way, we will stop immediately and stop it happening again.
4. If you think there is a mistake in your data, please tell us. You have a right to have it corrected. We may need to check what is the correct data, but will put right any mistakes as soon as possible.
5. Steamworks Learning remove your data after the booking has finished. You have a right for this to happen, because we do not need to keep your data any longer than this.

Appendix 5 - Request Form for Subject Access to Personal Data

Request for Access to Personal Data

Under the Data Protection Act 1998, you have the right to enquire of any organization whether they hold your personal data and to see a copy of that data. Individuals are called 'data subjects' in the Act.

If you require copies of data we may hold, please complete all sections below and return this form together with the necessary verification details. The information on the form will only be used to process your request and find information which relates to you. It will be kept on file to respond to any subsequent correspondence, and will not be used for any other purpose. A response will be provided within 14 days of receipt of the completed form and proof of identity.

1. Details of Person Requesting Information

Full Name:

Date of Birth:

Address:

Postcode:

Tel. No. Fax No. E-Mail

Other Address Details (if less than 3 years at above address)

Postcode:

4. Are You the Data Subject?

YES: If you are the Data Subject please supply evidence of your identity – passport, driving licence or birth certificate (originals only)

NO: Are you acting on behalf of the Data Subject with their written authority? If so, that authority must be enclosed.