SUPAJAM
GATEWAY TO MUSIC
MUSIC EDUCATION FOR 16 TO 25 YEAR OLDS

Ofsted
Good
Provider

Data Protection Policy

March 2022

(To be reviewed August 2022)

1. Introduction

This policy is intended to clarify data handling procedures for staff, to safeguard the personal data that SupaJam Education in Music and Media (SEMM) controls and processes, and to ensure compliance with the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR).

SEMM is registered with the Information Commissioner's Office (ICO) as a Data Controller under the Act and UK GDPR, and SEMM's CEO's are ultimately responsible for its implementation. Day to day responsibility for implementation is delegated to the Director of Education and Innovation, who is the Data Protection Lead (DPL).

It is essential that all staff are fully aware of this policy, and ensure that the protocols and procedures set out here are adhered to. If at any stage, a staff member feels that adequate guidance is not given within this policy, advice should be sought from in the first instance from the Data Protection Lead. The Data Protection Officer for SupaJam is Satswana (www.satswana.com).

2. The Data Protection Act 2018 and UK GDPR

The Data Protection Act 2018 and UK GDPR applies to personal information. This is data about living, identified or identifiable individuals and includes information such as names and addresses, bank details, images, biometrics (e.g. fingerprints) and opinions expressed about an individual. This includes verbal as well as written information. If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

Personal information can be processed only where at least one of the six lawful conditions applies:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear

basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

All personal data must be processed lawfully, fairly and in a transparent manner. The lawful basis for processing personal data must be clearly documented to demonstrate compliance. If no lawful basis applies to processing, it will be unlawful and in breach of the Act and UK GDPR.

Individuals, also known as Data Subjects, must be informed of the lawful basis for processing their data, how their data will be used, how their data will be securely stored and who, if applicable, their data will be shared with. This information must be provided at the earliest opportunity and must be clear and understandable. This is set out in SEMM's Privacy Notice, which is included in the onboarding process at the beginning of employment and which all staff are expected to be familiar with. Individuals also have the right to erase personal data which has been processed unlawfully.

2.1 Special Category Data

The Act and UK GDPR classifies some personal information as special category data because it is considered to be more sensitive and there are stricter rules about processing this category of information. For an outline of these rules, please see appendix 3.

The ten special categories of information are:

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sex life
- Sexual orientation.

Registration

SEMM is registered with the Information Commissioner's Office to process sensitive personal data, (Registration Number ZA168864). Our registration covers staff administration and the administration of student

records. Fuller details of what data SEMM may handle, and for what purpose, are given in Appendix 1.

Information about companies or public authorities is not personal data. However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information related to them as an individual may constitute personal data.

2.2 Data Protection Principles

Anyone processing personal data on behalf of SEMM must abide by the following principles:

- Personal data shall be processed fairly and lawfully. A lawful basis for processing shall be identified and recorded and processing of personal data shall not be unduly detrimental, unexpected or misleading to the data subjects involved.
- Personal data shall only be obtained for the specified lawful basis that is most appropriate and shall not be further processed in breach of any other laws.
- You must be clear, open and honest with people about how you will use their personal data.
- Data subjects shall be clearly and honestly informed of the lawful basis and the purpose of processing their personal data at the start or earliest opportunity in an understandable way. In most cases, SEMM's privacy policy can be used to provide this information.
- Personal data shall not be processed for a new purpose unless it is still compatible with the original purpose, consent is given, or there is a clear basis in law.
- Special category data shall only be processed for the lawful basis for general processing and the additional condition for processing this type of data.
- Only personal data that is 'necessary' shall be processed. If the same purpose can be reasonably achieved without processing the data then there is no lawful basis and personal data shall not be processed.
- Reasonable steps shall be taken to ensure personal data held is correct, is not misleading, and is kept updated if necessary for the purpose it is being used for. Reasonable steps shall be taken to correct or erase incorrect or misleading data as soon as possible after discovery.
- Personal data shall not be retained for longer than needed depending on the relevant lawful basis (See Appendix 2 for standard retention periods). Individuals have the right to erasure if the data is no longer needed.
- Personal data shall be processed in accordance with the rights of data subjects, ie with consent.
- Appropriate technical and organisational security measures shall be taken to protect the personal data held. Personal data shall not be transferred to

a country outside the European Economic Area unless adequate levels of protection exist.
- SEMM is responsible for the processing of personal data and shall have appropriate measures and records in place to be able to demonstrate compliance.

The definition of processing is wide, and covers almost any action carried out on a computer, electronic device, or in written, photographic or verbal format. The principles apply equally to data about SEMM's parents/guardians, volunteers, students, staff, and other stakeholders.

3. Responsibilities of Staff

Any staff who collect or process information about other people **must** comply with the principles and guidance set out in this Data Protection Policy. Failure to do so could result in disciplinary action, and at worst, unauthorised disclosure of sensitive personal data – whether intended or accidental – might constitute gross misconduct and could result in summary dismissal.

Please ensure you follow these guidelines, and seek advice from the DPL if you are in any doubt as to your responsibilities.

- Devices must be password protected (laptops, iPads, computers, phones, USB sticks, any other portable device)
- Devices must never be left unaccompanied in an unlocked space
- Desks must be clear and paperwork must be locked away
- Disposal of sensitive data should ensure information is shredded or permanently deleted
- Cookies should be cleared
- Passwords should be changed every 30 days
- Electronic information should be stored securely and for no longer than the required amount of time
- We recommend that all emails are deleted every 3 years as a minimum
- Data should be spot-checked for accuracy, particularly when data is being handled or entered in bulk
- Particular care should be taken with sensitive data obtained from third parties to ensure it is factual and not opinion, i.e. not from the data subject and not from within SEMM
- Managers should carry out periodic spot-checks to make sure that data being stored is still relevant and necessary.

3.1 The Role of the Data Protection Lead (DPL)

The DPL will:

- Carry out regular checks to ensure data is securely disposed of in line with Appendix 2 – Retention Guidelines

- Update the policy once a year
- Ensure all staff are trained in the UK GDPR
- Communicate with the DPO
- Audit all SupaJam bases
- Authorise access to SupaJam's CCTV systems

3.2 Keeping Data Secure

The main points to remember to ensure that data is kept secure are:

- Ensure that computer hardware is sited in a secure location
- Data must be stored on SEMM devices or approved ICT systems such as Arbor or Google Drive and not on personal devices
- Never leave electronic or paper data open or visible when you leave your desk, especially in public areas
- There must be a clear purpose for sharing data and the data must be limited to what is actually required. Reasonable steps must be taken to ensure the data is only shared with the appropriate individuals
- Always mark confidential information 'private and confidential for addressee only', and only send it to a named person who you know is entitled to receive it
- Always use a secure email address where possible; never email confidential information to generic or shared email addresses such as 'enquiry@...'
- Always check before forwarding emails or replying to all that everyone in the address list is entitled to receive the information being sent and only send information that is necessary to the purpose of the email
- When sending an email to a group of people, use the Bcc box to ensure that everyone's email addresses remain confidential
- If sending sensitive or personal information by post, check beforehand that you have the correct addressee and send it to that named person only Mark the envelope 'Addressee Only, Private and Confidential' and add a return address
- Always be aware of your environment when verbally sharing confidential information; who needs to know the information? Who else is present in the building and can see/hear information?
- Always politely challenge strangers encountered in the bases
- Take proper care with passwords that give you access to devices and IT systems
- Confidential waste must be disposed of securely. Certification confirming safe disposal is required whenever any hardware and software is disposed of and should be held by the DPL. Paper information must be cross shredded
- Keep files locked in secure cabinets when not in use
- Due to student files containing a large volume of personal data, these should not be sent through normal mail. If a file needs to be sent to another SEMM base this should be done electronically via a SEMM email address

- If you receive a telephone request for confidential personal information but you do not recognise the caller, do not give the information immediately. Check that the caller is someone who is entitled to the information and that any telephone number you are given by the caller is correct according to your records, then call back with the requested information. If you are unable to confirm the identity of the caller, speak to the DPL before providing any information
- If you are dealing with someone who is not personally known to you who makes a valid request for information in person, ask him or her to produce some evidence of identity before giving out the information, and remember to get the consent of the data subject
- When providing data subjects with a copy of information, ensure it has an electronic watermark
- If in doubt about whether or not to give out information – including to bodies such as the police and HM Revenue & Customs - please consult the DPL immediately, and always before disclosing data

Please note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

3.3 Handling Data away from SEMM Premises

It is understood that staff may need to access sensitive data away from SEMM premises e.g. when working from home or attending meetings. Reasonable steps must be taken to keep sensitive data secure and it should not be left in cars or be visible to others (e.g. when on public transport). If sensitive data is lost or compromised, this must be reported to the DPL, who will report it to the DPO immediately. SEMM has a responsibility to report a data breach to the ICO within 72 hours of becoming aware of it.

3.4 Sharing Personal Data within SEMM

Personal data should only be shared with other SEMM departments on a "need to know" basis, i.e. when it is needed for others to fulfil their official duties safely and effectively. Only the minimum amount of data required should be shared and information should be encrypted, anonymised or pseudonymised. Always send emails via SEMM's internal email system i.e. from one SEMM email address to another SEMM email address. If information is password protected, tell the recipient the password via telephone, do not send passwords in the same or subsequent emails. If sharing information verbally, make sure you are in a private area where you cannot be overheard by people who are not entitled to the information.

3.5 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise data protection risks of a project, for example opening a new base. SEMM must complete a DPIA for processing that is likely to result in a high risk to individuals. It is also good practice to complete a DPIA for any other major

project which requires the processing of personal data.

A DPIA must:

- Describe the nature, scope, context and purposes of the processing;
- Assess necessity, proportionality and compliance measures;
- Identify and assess risks to individuals; and
- Identify any additional measures to mitigate those risks.

The DPL must be informed of all DPIAs and they must be approved by the CEO's or an independent member of SLT before projects can commence. If you are unsure whether or not a DPIA is necessary, contact the DPL before proceeding with any new project.

SEMM will consult the ICO before starting any processing where a high risk that cannot be mitigated is identified.

4. Personal information access rights

The fundamental principle underlying the UK GDPR and Data Protection Act 2018 is that people should be able to know what is recorded about them. Most of the material which an individual sees on their file should already be familiar to them, since good practice will mean that records, work plans, and contracts would be shared at the time they are made.

The UK GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

4.1 Exclusions and limits to access

As stated above, SEMM aims to be transparent in its dealings with all stakeholders, and as a general principle will operate an open file policy which gives people free access to their records. However some restrictions do apply, and staff should follow these guidelines:

- ➔ a) Do not disclose personal information about an individual that includes information about a third person, without the consent of that third person
- ➔ b) Do not disclose personal information about an individual that

would identify a third person as its source, without the consent of that third person

- ➔ c) Consider whether disclosure is likely to result in serious harm to the data subject or to some other person. In such circumstances, access may be refused but the decision to withhold information for this reason may only be taken with the agreement of SLT in consultation with the DPO
- ➔ d) Information may be excluded if it is held for the purpose of prevention or detection of crime, or the apprehension of or prosecution of an offender
- ➔ e) Information can be withheld if it is a necessary and proportionate measure to safeguard public security and interests, in particular economic or financial interests; public health and security; the protection of judicial independence and proceedings; the protection of the individual, or the rights and freedoms of others; or the enforcement of civil law matters
- ➔ f) Any legal advice obtained about a data subject must not be disclosed without the agreement of the CEOs
- ➔ g) Children have the same rights as adults over their personal data, which they can exercise as long as they are competent to do so. Where a child is not considered to be competent, an adult with parental responsibility may usually exercise the child's data protection rights on their behalf. In the case of children, the DPL must be consulted and will decide if the child making the request for access understands the nature of the request. This will not be determined solely by the age of the child. If the child does not understand, the parent is entitled to make the request, and access will only be granted if SEMM is satisfied that the application is made in the child's best interests.
- ➔ h) Where applications are made on behalf of people suffering from a mental disorder who are deemed to lack mental capacity by a person acting under the order of the court of protection or in the terms of an enduring or Lasting Power of Attorney, or appointed as a Deputy by the court, staff should pass the request to the DPL who will consult with the DPO.

4.2 Procedure for making a SAR

Should you wish to make a subject access request and view the data that SupaJam holds on you, please contact the DPL. SARs are free of charge unless they are considered excessive.

They will acknowledge your request and inform you in writing of the date by which they will send you your personal information.

The DPL will be the central point for collating your data and will notify the CEOs.

They will work with the DPO to gather information from areas in which it has been stored.

There may be circumstances in which your access request is denied, where it is manifestly unfounded or excessive, or where personal data of another person is included alongside your own. In this situation, the DPL will consider whether this information can be redacted in order to comply with the request and to protect the data of the other person. In order to help with the SAR, the DPL may contact you to clarify what you need.

The DPL will have up to one month to send you your personal data. Should they require longer, they can request up to two months further and you will be informed of this within the first month.

Appendix 1

SEMM is registered with the ICO to process sensitive personal data, and our registration covers two work areas:

1. Staff administration
Data classes are: personal details, education and training, employment, financial, physical or mental health or condition, racial or ethnic origin, religious or other beliefs, and trade union membership.

Data subjects are: staff, volunteers, agency workers, temporary or casual workers; relatives, guardians and associates of the data subject; complainants, correspondents and enquirers.

2. Administration of student records
Data classes are: personal details, family lifestyle and social circumstances, financial details, goods or services provided, and membership.

Data subjects are: students.

Appendix 2 - Guidelines for Minimum Retention Time for Documents

HR		
Type of Data	**Retention Period**	**Reason for Retention**
Personnel Files; training records; notes of grievance and disciplinary hearings	6 years	Provision of references and limitation period for litigation
Staff Application forms; interview notes	6 months from the date of the interviews	Limitation period for litigation
Facts relating to redundancies (less than 20)	4 months from the date of redundancies	Limitation period for litigation
Facts relating to redundancies (20 or more)	6 months from the date of redundancies	Limitation period for litigation
DBS	6 months from the date of certificate receipt	Proof of suitability to work with vulnerable adults and children
Health Records	During Employment	Management of Health and Safety at Work Regulations
Health Records where reason for termination of employment is concerned with health, including stress-related illness	6 years	Limitation period for personal injury claims
Wages and salary records, expense accounts/records, overtime records/authoristation	6 years plus the current year	Taxes Management Act, Income Tax (Employment) Regulations 1993, National Minimum Wage Act 1998, The Working Time Regulations 1998
Redundancy details, calculation of payments, refunds, notifications to the Secretary of State	6 years after employment has ceased	Data Protection Act
Staff personnel charts	6 years after employment has ceased (records for key executives may be kept longer for historical purposes)	Limitation Act 1980
Applications for jobs – where the candidate was unsuccessful	6 months after notifying the unsuccessful candidate	Discrimination Acts 1975 and 1986 and Race Relations Act 1976 recommend 6 months. One year limitation for defamation actions under Limitations Act
Statutory Maternity [paternity] Pay records and calculations or other medical evidence	3 years after the end of the tax year in which the maternity period ends	Statutory Maternity Pay (General) Regulations 1986
Sickness records	6 years	Statutory Sick Pay (General) Regulations 1982

Health & Safety records	3 years for general records. Permanently for records relating to hazardous substances	Personal injury actions must generally be commenced within three years of injury. However industrial injuries not capable of detection within that period (i.e. Asbestos) the time period may be substantially extended.
Volunteers		
Type of Data	**Retention Period**	**Reason for Retention**
Application forms, references, and associated documents.	3 years	So that references can be given if needed.
Health & Safety		
Type of Data	**Retention Period**	**Reason for Retention**
Medical Records kept by reason of the Control of Substances Hazardous to Health Accident Books, Records and reports of accidents.	40 years 3 years after the date of the last entry	COSHH Regulation 1994 RIDDOR 1985
Hazardous substances: disposal of heavy materials and radioactive sources	Permanently	Data Protection Act
Records of major refurbishments, warranties, planning consents, design documents, final health and safety files	13 years for actions against contractors etc.	Data Protection Act
Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations 1999	5 years from the date on which the tests were carried out	Control of Substances Hazardous to Health Regulations 1999 (COSHH) (SI 1999/437)
Medical Records and details of biological tests under the Control of Lead at Work Regulations 1998	40 years from the date of the last entry	Control of Lead at Work Regulations 1998(SI 1998/543)
Medical records as specified by the Control of Substances Hazardous to Health Regulations 1999	40 years from the date of the last entry	Control of Substances Hazardous to Health Regulations 1999 (COSHH) (SI 1999/437)
Finance		
Type of Data	**Retention Period**	**Reason for Retention**

Bank paying in counterfoils; bank statements; remittance advices; correspondence re donations; bank reconciliations; instructions to banks	6 six years from the end of the financial year in which the transaction was made	Companies Act/Charities Act
Receipts cash book; sales ledger	10 years	Companies Act/Charities Act and HMRC
Payments cash book or record of payments made; purchase ledger; invoice – revenue; petty cash records	6 years from the end of the financial year in which the transaction was made	Companies Act/Charities Act and HMRC
Purchase invoice – capital item	10 years	Companies Act/Charities Act and HMRC
Management accounts	6 years	Companies Act/Charities Act and HMRC
Annual accounts and annual review	Permanently	Data Protection Act
Investment certificates	Permanently	Companies Act, charities Act, commercial
Investment ledger; fixed assets register	Permanently	Companies Act, charities Act, commercial
Deeds of title	Permanently or until property is disposed of (copy of title deeds should be kept for 6 years after disposal)	Data Protection Act
Leases	15 years after expiry	Limitations Act 1960
Final plans, designs and drawings of the building, planning consents, building certifications, collateral warranties, records of historical interest and final health and safety file.	Permanently or until 6 years after property is disposed of	Data Protection Act

Payroll		
Type of Data	**Retention Period**	**Reason for Retention**
Income Tax and NI returns; correspondence with Tax Office	3 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Sick Pay records and calculations	3 years after the end of the financial year to which the records relate	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years from the last date of employment	Taxes Management Act 1970

Income tax records re employees leaving i.e. P45; notice to employer of tax code (P6); annual return of employees and directors expenses and benefits (PD11); certificate of pay and tax deducted (P60); Notice of tax code change; annual return of taxable pay and tax deducted.	6 years plus current year	Taxes Management Act
Records of pension deductions (including superannuation)	6 years plus current year	Pensions act 1995
Payroll and payroll control account	6 years plus current year	Companies Act/Charities Act and Taxes Management Act
Pensions		
Type of Data	**Retention Period**	**Reason for Retention**
Details re: current pensioners	12 years after benefit ceases	Commercial
Pensions scheme – next of kin/ expression of wish forms	6 years after date of death	Data Protection Act
All trust deeds and rules; Trustees' minute book; annual accounts; Investment and insurance policy records; Actuarial reports; Contribution.	Permanently	Companies Act, Commercial, Pensions Act 1995
Insurance		
Type of Data	**Retention Period**	**Reason for Retention**
Policies	10 years after lapse	Data Protection Act
Claims correspondence; accident reports and relevant correspondence	3 years after settlement	Data Protection Act
Employer's Liability Insurance Certificate Public Liability Insurance Certificate.	40 years	Employers' Liability (Compulsory Insurance) Regulations 1998
Students		
Type of Data	**Retention Period**	**Reason for Retention**
Manual (paper) files such as: name and address, academic achievements including marks for course work, copies of any references given.	7 years after the student has left SEMM	Data Protection Act
Information kept on computerised systems.	10 years after the student has left SEMM	Data Protection Act
General		

Type of Data	Retention Period	Reason for Retention
Advisory Board meetings minutes and decisions	Permanently	Companies House
SLT meetings minutes and decisions	Permanently	Companies House
Register of directors & secretaries	Permanently	Companies House
Certificate of Incorporation	Permanently	Companies House
Contract with suppliers or agents, licensing agreements, rental/hire purchase agreements, indemnities and guarantees and other agreements or contracts	6 years after expiry or termination of the contract. If the contract is executed as a deed, the limitation period is 12 years.	Limitations Act 1980

Appendix 3 - Conditions for processing special category data

The conditions are listed in Article 9(2) of the UK GDPR:

- (a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- (b) Processing is necessary for the purposes of: carrying out the obligations and exercising specific rights (of the controller or of the data subject) in the field of employment, social security and social protection law. This is in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law, providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- (c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- (d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- (e) Processing relates to personal data which are manifestly made public by the data subject;
- (f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- (g) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- (h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- (i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- (j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data.