ISCA
INTERNATIONAL SCHOOL OF CREATIVE ARTS

International School of Creative Arts

Data Protection Policy

Need a large print copy?

Please ask in the School Office.

Control Page

Document Title	Data Protection Policy	
Document Reference	ISCA 23	
Version	5.0	21/07/2023
Author	Executive Director	
Location	J:\9. POLICIES AND PROCEDURES\Approved	
Controller	Head of School	
Approved	Senior Management Team	
Date of Adoption	September 2023	
Date of Next Review	September 2024	

Contents

Introduction

The School is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR) and all other data protection legislation currently in force. The Regulation applies to anyone processing personal information (data) or sensitive personal information (or data) and sets out principles which should be followed and gives rights to those whose data is being processed.

This policy sets out how we comply with our data protection obligations and seeks to protect personal information relating to our workforce. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

The policy applies to all personal data, regardless of whether it is in paper or electronic format.

Definitions

Personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information
Sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.
Criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures
Processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it
Data subject	means the individual to whom the personal information relates
Data processor	a person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller
Data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information

Roles and Responsibilities

Data Controller

The school and its employees keep and process personal data relating to parents, students, staff, contractors, visitors and others and therefore is a data controller

The school is registered as a data controller with the ICO (Ref Z1781895) and will renew this registration annually or as otherwise legally required.

Data Protection Officer

The Operations Manager is responsible for data protection compliance and implementation within the organisation. If you have any questions or comments about the content of this policy or if you need further information, you should contact the Operations Manager by email i.ancuta@isca.uk.com or by telephone on 01753 208820.

All Staff & Contractors

All members of staff, contractors engaged by the School and data users on behalf of the data controller are responsible for:

- Collection, storing and processing any personal data in accordance with this policy.
- Contacting the Data Protection Officer
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - If they have any concerns that this policy is not being followed.
    - If they are unsure whether they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
    - If there has been a data breach.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
    - If they need help with any contracts or sharing personal data with third parties.

Anyone who has access to personal information must:

- only access the personal information that they have authority to access, and only for authorised purposes;
- only allow other School staff to access personal information if they have appropriate authorisation;
- only allow individuals who are not School staff to access personal information if you have specific authority to do so from the Operations Manager;
- keep personal information secure e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Data Security section of this policy.
- not remove personal information, or devices containing personal information (or which can be used to access it), from the School's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
- not store personal information on local drives or on personal devices that are used for work purposes.

Training

The School will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure. Training is provided through in-house or external provision as updates to the law occur.

Data protection principals

The School endorses fully and adheres to the Data Protection Principles listed below. When processing data we will ensure that it is:

- Processed lawfully, fairly and in a transparent way ('lawfulness, fairness and transparency'); and
- Processed no further than the legitimate purposes for which that data was collected ('purpose limitation'); and
- Limited to what is necessary in relation to the purpose ('data minimisation'); and
- Accurate and kept up to date ('accuracy'); and
- Kept in a form which permits identification of the data subject for no longer than is necessary ('storage limitation'); and
- Processed in a manner that ensures security of that personal data ('integrity and confidentiality'); and
- Processed by a controller who can demonstrate compliance with the principles ('accountability').

Rights for Data Subjects

These rights must always be observed when processing or using personal information.

Data subjects have the following rights in relation to their personal information:

- to be informed about how, why and on what basis that information is processed—see the School's data protection privacy notice;
- to obtain confirmation that their information is being processed and to obtain access to it and certain other information, by making a subject access request—see the School's subject access request;
- to have data corrected if it is inaccurate or incomplete;
- to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');
- to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal

information but you require the data to establish, exercise or defend a legal claim; and

- to restrict the processing of personal information temporarily where they do not think it is accurate (and the employer is verifying whether it is accurate), or where they have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

If a data subject wishes to exercise any of the rights in paragraphs above, they should contact the Operations Manager**.**

Basis for Processing Personal Information

Through appropriate management and strict application of criteria and controls, the School will:

- observe fully the conditions regarding having a lawful basis to process personal information
- meet its legal obligations to specify the purposes for which information is used
- ensure the individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent
- ensure that the processing is necessary for the protection of the vital interests of the data subject or another natural person
- collect and process appropriate information only to the extent that it is necessary to fulfil contractual or operational needs or to comply with any legal requirements
- ensure the information held is accurate and up to date
- ensure that the information is held for no longer than is necessary
- ensure that the rights of people about whom information is held can be fully exercised under the GDPR (i.e. the right to be informed that processing is being undertaken, to access personal information on request; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information)
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred outside the EU, to third countries or international organisations without an adequate level of protection.
- only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
- ensure that if we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.
- make sure staff must only process personal data where it is necessary in order to do their jobs.
- instruct staff that if they no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Storage and Deletion of data guidelines within this policy document.

- include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);
- where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

Personal information

Employees

Throughout employment and for as long as is necessary after the termination of employment, the School will need to process data about people working for it.

We may collect the following information about employees:

- their name, contact details (i.e. address, home and mobile phone numbers, email address) and emergency contacts (i.e. name, relationship and home and mobile phone numbers)
- information collected during the recruitment process that we retain during their employment
- employment contract information
- details of salary and benefits, bank/building society, National Insurance and tax information, your age
- details of their spouse/partner and any dependants
- their nationality and immigration status and information from related documents, such as their passport or other identification and immigration information
- a copy of your driving licence if available
- details of pension arrangements, and all information included in these and necessary to implement and administer them
- information in their sickness and absence records (including sensitive personal information regarding their physical and/or mental health)
- racial or ethnic origin, sex and sexual orientation, religious or similar beliefs
- criminal records information, including the results of Disclosure and Barring Service (DBS) checks
- information on grievances raised by or involving them
- information on conduct and/or other disciplinary issues involving them
- details of appraisals and performance reviews
- details of performance management/improvement plans (if any)
- details of time and attendance records
- information in applications made for other positions within our organisation
- information about use of our IT, communication and other systems, and other monitoring information
- their image, in photographic and video form
- details of their use of business-related social media, such as LinkedIn

- use of public social media (only in very limited circumstances, to check specific risks for specific functions within our organisation; they will be notified separately if this is to occur)
- details in references about them that we give to others

Certain of the categories above may not apply if the data subject is an independent contractor, freelancer or intern.

Recruitment process:

The HR department, with guidance from the Operations Manager will ensure that (except where the law permits otherwise):

- during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, e.g. race or ethnic origin, trade union membership or health
- if sensitive personal information is received, e.g. the applicant provides it without being asked for it within his or her CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted
- any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision
- 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages
- we will only ask health questions once an offer of employment has been made
- CRB/DBS checks are carried out as a condition of employment and adhering to the Safeguarding policy

During employment:

The HR department, with guidance from the Operations Manager, will process:

- health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits
- sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting (where possible, this information will be anonymised);
- trade union membership information for the purposes of staff administration and administering 'check off'
- CRB/ DBS checks (these are kept on file and regularly kept up to date but not applied for more than annually unless there is a reason for doing so and the employee is informed)

Students

Throughout their studies at the School and for as long as is necessary after students leave, the School will need to process data about them. This is set out in the Storage and Deletion of Data section within this policy.

We may collect the following information during their courses:

- name, contact details (i.e. address, home and mobile phone numbers, email address) and emergency contacts (i.e. name, relationship and home and mobile phone numbers);
- information collected during the recruitment process that we retain whilst they are a student including any academic references and documentation obtained during the application process
- information about their age
- nationality and immigration status and information from related documents, such as passport or other identification and immigration information
- information in sickness and absence records (including sensitive personal information regarding physical and/or mental health)
- passport and immigration information where relevant
- details of health and sickness records
- details about Special Educational Needs if relevant
- details arising out of safeguarding issues if relevant
- information about performance, behaviour and academic progress, including examination results
- details of any behavioural investigations and any actions taken.
- financial details about fees and payments
- correspondence with the School and other information that they have given to the School
- details of attendance records
- information in applications made for other courses within the school
- information about their use of our IT, communication and other systems, and other monitoring information
- their image, in photographic and video form, including from CCTV footage
- details in references about them that we give to others

Visitors

Information on visitors entering and leaving the site will be captured by Security staff of Teikyo School. They are the data controller for this information. Images from CCTV managed by Teikyo may also be captured by them.

The data we will hold about a visitor may include:

- date visited, with time of arrival and departure
- badge number issued by Teikyo Security staff
- name of Visitor
- company Visitor belongs to
- car registration

Information will be given by the Visitor in the visitors' signing in book held in reception.

Once each page of the book is complete, this will be stored in a locked drawer or cupboard for a period of 12 months and then destroyed in accordance with the Deletion of Data section in this policy.

If a visitor connects to the school Wi-Fi we may collect the following data:

- device name,
- mac address,
- browsing history

A privacy notice will be made available to each visitor on signing in at the Office.

Sensitive Personal Information

Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.

The School may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

- we have a lawful basis for doing so as set out above, e.g. it is necessary for the performance of the employment contract, to comply with the School's legal obligations or for the purposes of the School's legitimate interests; and
- one of the special conditions for processing sensitive personal information applies, e.g.:
    - the data subject has given explicit consent
    - the processing is necessary for the purposes of exercising the employment law rights or obligations of the School or the data subject
    - the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
    - processing relates to personal data which are manifestly made public by the data subject
    - the processing is necessary for the establishment, exercise or defence of legal claims; or
    - the processing is necessary for reasons of substantial public interest.

Before processing any sensitive personal information, staff must notify the Operations Manager of the proposed processing, in order that the Operations Manager may assess whether the processing complies with the criteria noted above. Sensitive personal information will not be processed until this is sought and the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

The School will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

The School's data protection privacy notice sets out the types of sensitive personal information that the School processes, what it is used for and the lawful basis for the processing.

Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- there is an issue with a student or parent/carer that puts the safety of our staff at risk
- we need to liaise with other agencies – we will seek consent as necessary before doing this
- our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
    - only appoint suppliers or contractors which can provide guarantees that they comply with data protection law
    - establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- the prevention or detection of crime and/or fraud
- the apprehension or prosecution of offenders
- the assessment or collection of tax owed to HMRC
- HM Immigration Services, where the data subject requires the school to sponsor their visa application
- in connection with legal proceedings
- where the disclosure is required to satisfy our safeguarding obligations
- research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

CCTV Systems

The School's landlord, Teikyo School, may capture images from its CCTV system for the safety and security of Staff, Students and Visitors. Please see appendices for a copy of Teikyo School CCTV policy.

Subject Access Request to Data

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- confirmation that their personal data is being processed

- access to a copy of the data
- the purposes of the data processing
- who the data has been, or will be, shared with
- the source of the data, if not the individual
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the Data Protection Officer. They should include:

- name of individual
- correspondence address
- contact number and email address
- details of the information requested

If staff receive a subject access request they must immediately forward it to the Data Protection Officer.

Students and subject access requests

Personal data about a student belongs to that student, and not the student's parents or guardian. Access requests can be made by parents or guardians for students under 18 years old.

Responding to subject access requests

When responding to requests, we:

- may ask the individual to provide 2 forms of identification
- may contact the individual via phone to confirm the request was made
- will respond without delay and within 1 month of receipt of the request
- will provide the information free of charge
- may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or onerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- might cause serious harm to the physical or mental health of the student or another individual
- would reveal that the student is at risk of abuse, where the disclosure of that information would not be in the student's best interests
- is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- withdraw their consent to processing at any time
- ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- prevent use of their personal data for direct marketing
- challenge processing which has been justified on the basis of public interest
- request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- prevent processing that is likely to cause damage or distress
- be notified of a data breach in certain circumstances
- make a complaint to the ICO
- ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Data Protection Officer. If staff receive such a request, they must immediately forward it to the Data Protection Officer.

Data Security

The School will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

- making sure that, where possible, personal information is pseudonymised or encrypted;
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing
- paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/ display boards, or left anywhere else where there is general access

- where personal information needs to be taken off site, staff must sign it in and out from the school office
- passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- mobile phones are to be password protected and contain software to erase data, should the device be lost or stolen
- USB devices are not permitted except where it is required by students for examination purposes, such as an portfolio examination.
- staff or students or who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.

Where the School uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- the organisation may act only on the written instructions of the School;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent of the School and under a written contract;
- the organisation will assist the School in providing subject access and allowing individuals to exercise their rights under the GDPR;
- the organisation will assist the School in meeting its GDPR obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the organisation will delete or return all personal information to the School as requested at the end of the contract; and
- the organisation will submit to audits and inspections, provide the School with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the School immediately if it is asked to do something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Operations Manager**.**

Data Breaches

A data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;

- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

The School will:

- make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

See Appendix 2 for a full description of ISCA's data breach procedure.

Storage and Deletion of Data

Data is stored in line with our retention and disposal schedule (see Appendix 1).

The school will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide guarantees and certification that it complies with data protection law.

Consequences of failing to comply

The School takes compliance with this policy very seriously. Failure to comply with the policy:

- puts at risk the individuals whose personal information is being processed;
- carries the risk of significant civil and criminal sanctions for the individual and the School; and
- may, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Email: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk

ISCA
INTERNATIONAL SCHOOL OF CREATIVE ARTS

Appendix 1

Retention and Disposal Schedule

Management & Organisation

Record	Minimum Retention Period	Action After Retention
Senior Management Team-Meeting Minutes	Current academic year + 6 years	Archive for Permanent Preservation
Staff Meeting Minutes	Academic year + 6 years	Destroy
School Development Plan	Retain in School for 10 years from closure of Plan	Archive for Permanent Preservation
Policies	Retain while current. Retain 1 copy of old policy for 2 years after being replaced	Destroy
Visitors Book	Current academic year + 6 years	Destroy
Circulars to Staff, Parents and Students	Current academic year + 3 years	Destroy
School Brochures/ Prospectus	Current academic year + 3 years	Destroy
Complaints	25 years from the date the school becomes aware.	Destroy
Annual Report	Retain in School for 10 years from date of Report	Archive for Preservation

Legislation and Guidance from DE, ELB, ESA, CCMS etc

Record	Minimum Retention Period	Action After Retention
Circulars, Guidance, Bulletins from DE, ELB etc	Until superseded	Destroy
Correspondence re: Statistical Returns to DE, ELB etc	Current financial year + 6 years	Destroy
DE Reports, Inspections	Until superseded	Destroy

Students

Record	Minimum Retention Period	Action After Retention
Student Admission Data		
Applications for enrolment	3 years after enrolment	Destroy
Transfer applications (Transfer Forms)	3 years after enrolment	Destroy
Student Attendance Information/Registers	Date of Register + 10 years	Archive for Preservation
Student Education Records		
School/Progress Reports etc.	Until student is 23 years old	Destroy
School/Progress Reports etc. (Special Educational Needs)	Until student is 26 years old	Destroy
Child Protection Information		
Record of concerns where case was not referred to Social	10 years after last entry on file	Destroy

Record	Minimum Retention Period	Action After Retention
Services		
Social Services investigation outcome was unfounded or malicious	10 years after last entry on file	Destroy
Social Services investigation outcome was inconclusive, unsubstantiated or substantiated	Until student is 30 years old	Destroy
Disciplinary Action		
(Suspension/Expulsion)/Offences – bullying	Until student is 23 years old	Destroy
(Suspension/Expulsion)/Offences – bullying (Special Educational Needs)	Until student is 26 years old	Destroy
Trips		
Financial & Administration details	Current financial year + 6 years	Destroy
Attendance/Staff Supervision etc.	Current financial year + 6 years. In the case of an incident/accident involving a student, retain until student is 23 years old or 26 for a student with special educational needs	Destroy
Medical Records		
Records of Students with medical conditions and details for the administration of drugs when necessary.	Until student is 23 years old or in the case of a Special Needs Student, until 26 years old	Destroy
Other		
Timetables + Class Groupings	Retain while current	Destroy
Examination Results	Current school year + 6 years	Destroy
Careers Advice	Current school year + 6 years	Destroy
Reports of Stolen/Damaged Items	Current financial year + 6 years	Destroy

Staff

Record	Minimum Retention Period	Action After Retention
Staff Personnel Records (including, appointment details, training, staff development etc.)	7 years after leaving employment	Destroy
Interview notes and recruitment records	Date of interview + 6 months	Destroy
Staff Salary Records	7 years after leaving employment	Destroy
Staff Sickness Records (copies of Medical Certs)	Current school year + 6 years	Destroy
Substitute Staff Records-non teaching	Current school year + 6 years	Destroy
Student Records-non teaching	Current school year + 6 years	Destroy
Procedures for Induction of Staff	Until superseded	Destroy
Staff/Teachers' Attendance Records	7 years after leaving	Destroy

Record	Minimum Retention Period	Action After Retention
Staff Performance Review	7 years after leaving	Destroy
Child Protection records relating to an Independent Inquiry into Child Sexual Abuse where the outcome was inconclusive, unsubstantiated or substantiated.	All records should be retained at least until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer.	Destroy

Finance

Record	Minimum Retention Period	Action After Retention
Annual budget and budget deployment	Current financial year + 6 years	Destroy
Budget Monitoring	Current financial year + 6 years	Destroy
Annual Statement of Accounts (Outturn Statement)	Current financial year + 6 years	Destroy
Order Books, Invoices, Bank Records, Cash Books, Till Rolls, Lodgement books etc.	Current financial year + 6 years	Destroy
Postage Book	Current financial year + 6 years	Destroy
Audit Reports	Current financial year + 6 years	Destroy

Health & Safety

Record	Minimum Retention Period	Action After Retention
Accident Reporting (Adults)	Date of incident + 7 years	Destroy
Accident Reporting (Children)	Until student is 23 years old or in the case of a Special Needs student, until 26 years old	Destroy
Risk Assessments – work experience locations / students	7 years	Destroy
H & S Reports	15 years	Destroy
Fire Procedure	Until superseded	Destroy
Security System File	For the life of the system	Destroy

Appendix 2

Data Breach Procedure

Policy Statement

ISCA holds records of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This breach procedure applies to all personal and sensitive data held by ISCA.

This procedure applies to all school staff.

Purpose

This breach procedure sets out the course of action to be followed by all staff at ISCA if a data protection breach takes place.

Legal Context

The Data Protection Act 1998 makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

Principle 7 of the Act states that organisations which process personal data must take “appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”.

Types of Breach

ISCA takes breaches of security seriously. Examples of potential breaches of security can be caused by a number of factors. Some examples are:

Loss or theft of student, staff data and/ or equipment on which data is stored;

- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Human Error;
- Unforeseen circumstances such as fire or flood;
- Hacking;
- ‘Blagging’ offences where information is obtained by deception.

Immediate Containment/Recovery

In discovery of a data protection breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the Operations Manager. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Operations Manager must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.
3. As a registered Data Controller, it is ISCA's responsibility to take the appropriate action and conduct any investigation.
4. The Operations Manager must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.
5. The Head of Operations must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:
    - Attempting to recover lost equipment.
    - Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual making the enquiry back.
    - Whatever the outcome of the call, it should be reported immediately to the Operations Manager
    - The use of back-ups to restore lost/damaged/stolen data. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
    - If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Operations Manager to fully investigate the breach. They should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation.

The investigation should consider:

- type of data;
- Its sensitivity;
- What protections are in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (students, staff members, suppliers etc) and whether there are wider consequences to the breach.

- A clear record should be made of the nature of the breach and the actions taken to mitigate it.

The investigation should be completed as a matter of urgency and, wherever possible, within five days of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an investigation has taken place. The Operations Manager should, after seeking expert or legal advice, decide whether anyone should be notified of the breach.

In the case of significant breaches, the Information Commissioner's Office (ICO) should be notified. Incidents should be considered on a case by case basis. The following points will help you to decide whether and how to notify:

- Are there any legal/contractual requirements to notify?
- Will notification help prevent the unauthorised or unlawful use of personal data?
- Could notification help the individual – could they act on the information to mitigate risks?

If a large number of people are affected, or there are very serious consequences, you should notify the ICO. The ICO should only be notified if personal data is involved. There is guidance available from the ICO on when and how to notify them, which can be obtained at: http://www.ico.gov.uk/for_organisations/data_protection/the_guide/~/media/documents/library/Data_Protection/Practical_application/breach_report ing.ashx.

Consider the dangers of over-notifying. Not every incident warrants notification and over-notification may cause disproportionate enquiries and work. The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach. When notifying individuals, give specific and clear advice on what they can do to protect themselves and what you are willing to do to help them.

You should also give them the opportunity to make a formal complaint if they wish following the School's Complaints Procedure.

Review and Evaluation

Once the initial aftermath of the breach is over, the Operations Manager should fully review both the causes of the breach and the effectiveness of the response to it. It should be written and sent to the next available management team meeting for discussion.

If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right.

If the breach warrants a disciplinary investigation, the manager leading the investigation should do so in line with ISCA's Disciplinary Procedure and Policy.

This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance. Consideration should be given to reviewing this breach procedure whenever the data protection policy is reviewed.

Implementation

ISCA will ensure that staff are aware of the Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction and supervision. If staffs have any queries in relation to the policy, they should discuss this with the Operations Manager.

Appendix 3

Teikyo School CCTV Policy

Revision and Terminology

Please refer to the Policies Review Schedule, or in line with any changes in regulations.

Owner:	Bursar
Version Number:	1
Working Date:	22 June 2018
Statutory Policy? / Other Policy?	Other
Authorised by:	General Manager
Effective date of Policy:	22 June 2018
Circulation:	All Staff and Parents
Status:	

Contents

The purpose of this policy is to regulate the management and operation of the Closed Circuit Television (CCTV) System at Teikyo School UK (the **School**). It also serves as a notice and a guide to data subjects (including students, parents, staff, volunteers, visitors to the School and members of the public) regarding their rights in relation to personal data recorded via the CCTV system (the **System**).

The System is administered and managed by the School, who act as the Data Controller. This policy will be subject to review from time to time, and should be read with reference to the School Privacy Notice. For further guidance, please review the Information Commissioner's CCTV Code of Practice (https://ico.org.uk/media/1542/cctv-code-of-practice.pdf).

All fixed cameras are in plain sight on the School premises and the School does not routinely use CCTV for covert monitoring or monitoring of private property outside the School grounds.

The School's purposes of using the CCTV system are set out below and, having fully considered the privacy rights of individuals, the School believes these purposes are all in its legitimate interests. Data captured for the purposes below will not be used for any commercial purpose.

1. OBJECTIVES OF THE SYSTEM

1.1 To protect students, staff, volunteers, visitors and members of the public with regard to their personal safety.

1.2 To protect the School buildings and equipment, and the personal property of students, staff, volunteers, visitors and members of the public.

1.3 To support the police and community in preventing and detecting crime, and assist in the identification and apprehension of offenders.

1.4 To monitor the security and integrity of the School site and deliveries and arrivals, including car parking.

1.5 To monitor staff and contractors when carrying out work duties.

1.6 To monitor and uphold discipline among students in line with the School Rules, which are available to parents and students on request.

2. POSITIONING

2.1 Locations have been selected, both inside and out, that the School reasonably believes require monitoring to address the stated objectives.

2.2 Adequate signage has been placed in prominent positions to inform staff and students that they are entering a monitored area, identifying the School as the Data Controller and giving contact details for further information regarding the system.

2.3 No images will be captured from areas in which individuals would have a heightened expectation of privacy, including changing and washroom facilities.

2.4 No images of public spaces will be captured except to a limited extent at site entrances.

3. MAINTENANCE

3.1 The CCTV System will be operational 24 hours a day, every day of the year.

3.2 The System Manager (defined below) will check and confirm that the System is properly recording and that cameras are functioning correctly, on a regular basis.

3.3 The System will be checked and (to the extent necessary) serviced no less than annually.

4. SUPERVISION OF THE SYSTEM

4.1 Staff authorised by the School to conduct routine supervision of the System includes security staff, teaching, and administrative staff.

4.2 Images will be viewed and/or monitored in a suitably secure and private area to minimise the likelihood of or opportunity for access to unauthorised persons.

5. STORAGE OF DATA

5.1 The day-to-day management of images will be the responsibility of the Bursar who will act as the System Manager, or such suitable person as the System Manager shall appoint in his or her absence.

5.2 Images will be stored for four weeks, and automatically over-written unless the School considers it reasonably necessary for the pursuit of the objectives outlined above, or if lawfully required by an appropriate third party such as the police or local authority.

5.3 Where such data is retained, it will be retained in accordance with the Act and our Data Protection Policy. Information including the date, time, and length of the recording, as well as the locations covered and groups or individuals recorded, will be recorded in a system log book.

6. ACCESS TO IMAGES

6.1 Access to stored CCTV images will only be given to authorised persons, under the supervision of the System Manager, in pursuance of the above objectives (or if there is some other overriding and lawful reason to grant such access).

6.2 Individuals also have the right to access personal data the School holds on them (please see the School Privacy Notice and Data Protection Policy), including information held on the System, if it has been kept. The School will require specific details including at least to time, date and camera location before it can properly respond to any such requests. This right is subject to certain exemptions from access, including in some circumstances where others are identifiable.

6.3 The System Manager must satisfy themselves of the identity of any person wishing to view stored images or access the system and the legitimacy of the request. The following are examples when the System Manager may authorise access to CCTV images:

6.3.1 where required to do so by the Head, the General Manager, the Police or some relevant statutory authority;

6.3.2 to make a report regarding suspected criminal behaviour;

6.3.3 to enable the Designated Safeguarding Lead(s) or his/her appointed deputy to examine behaviour which may give rise to any reasonable safeguarding concern;

6.3.4 to assist the School in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardian will be informed as part of the School's management of a particular incident;

6.3.5 to data subjects (or their legal representatives) pursuant to an access request under the Act and on the basis set out in 6.2 above;

6.3.6 to the School's insurance company where required in order to pursue a claim for damage done to insured property; or

6.3.7 in any other circumstances required under law or regulation.

6.4 Where images are disclosed under 6.3 above a record will be made in the system log including the person viewing the images, the time of access, the reason for viewing the images, the details of images viewed and a crime incident number (if applicable).

7. OTHER CCTV SYSTEMS

7.1 The School does not own or manage third party CCTV systems, but may be provided by third parties with images of incidents where this in line with the objectives of the School's own CCTV policy and/or its School Rules.

7.2 Students often travel to School trips on coaches provided by third party contractors and a these coaches may be equipped with CCTV systems. The School may use these in establishing facts in cases of unacceptable student behaviour, in which case the parents/guardian will be informed as part of the School's management of a particular incident.

8. COMPLAINTS AND QUERIES

8.1 Any complaints or queries in relation to the School CCTV system, or its use of CCTV, or requests for copies, should be referred to the Bursar.

8.2 For any other queries concerning the use of your personal data by the School, please see the School Privacy Notice.