PORG International School GDPR & Data Protection Policy

Prepared by:	Barbora Gazdova	Date: August 2024
Last update by:	Barbora Gazdova	Date: August 2026
Approved by:	Dagmar Dluhosova	

Content

INTRODUCTION **4**
PURPOSE **4**
AIM **5**
LEGAL FRAMEWORK **6**
SCOPE **6**
DEFINITION **6**

Personal Data 6
Special Category Data 7
Processing 7

DATA PROTECTION PRINCIPLES **8**
TYPES OF DATA PROCESSES **8**
LAWFUL BASES FOR PROCESSING **8**
CHILDREN'S DATA **8**
DATA SHARING **9**
INTERNATIONAL DATA TRANSFER **11**
DATA RETENTION **12**
INFORMATION SECURITY **14**

Technical Security Measures 14
Organisational Security Measures 15
Remote Working and Mobile Devices 15
Physical Security 16
Data Breach and Cybersecurity Incident Management 16
Third-Party Security 16
Staff Awareness and Training 17

USE OF PHOTOGRAPHY AND VIDEO **17**

Consent Requirements 18
Safeguarding Considerations 18
Appropriate Use by Staff 18
Educational and Observation Use 19
Security and CCTV 19
Storage and Retention 19
Third-Party Platforms and Publications 20

CCTV **20**

Purpose of CCTV Monitoring 20
Scope and Location of CCTV 21
Transparency and Signage 21
Access and Confidentiality 21
Retention and Storage 22
Data Subject Rights 22
Sharing of CCTV Footage 23
Security and Monitoring 23
Safeguarding and Child Protection 23

DATA SUBJECT RIGHTS **24**
DATA BREACHES **24**

Immediate Response 25
Investigation and Risk Assessment 25
Notification Obligations 25
Containment and Mitigation 26

Record Keeping 26
Staff Responsibilities and Training 27
Safeguarding Considerations 27

STAFF RESPONSIBILITIES 27

Confidentiality Obligations 28
Use of School Systems and Technology 28
Training and Awareness 29
Reporting Responsibilities 29
Non-Compliance 29

DATA PROTECTION GOVERNANCE 30
COMPLAINTS 30
POLICY REVIEW AND PUBLICATION 32
KEY CONTACTS 32

Introduction

PORG International School – Primary & EYFS Division is committed to maintaining the highest standards of privacy, confidentiality, safeguarding, and responsible information management. As an educational institution working closely with children, families, employees, and external partners, the School recognises its obligation to protect personal data and ensure that all information is processed lawfully, fairly, transparently, and securely.

This GDPR & Data Protection Policy establishes the principles and procedures governing the collection, use, storage, sharing, retention, and protection of personal data within the School. The policy reflects the School's commitment to compliance with Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR), Czech data protection legislation, safeguarding obligations, and best practices expected within international educational environments and the British School Overseas (BSO) framework.

The School acknowledges that children's data requires enhanced protection, particularly within the Early Years Foundation Stage (EYFS) and Primary School settings. All staff, contractors, volunteers, and third parties acting on behalf of the School are therefore expected to handle personal data responsibly, confidentially, and in accordance with this policy.

The purpose of this policy is to:

- protect the rights and privacy of pupils, parents, employees, and members of the school community,
- ensure lawful and secure processing of personal data,
- support safeguarding and child protection responsibilities,
- minimise risks associated with data breaches and misuse of information,
- establish clear responsibilities for data protection compliance across the School.

This policy applies to all personal data processed by the School in both electronic and paper formats and forms part of the School's wider safeguarding, governance, and compliance framework.

Purpose

PORG International School ("the School") is committed to protecting the privacy, confidentiality, integrity, and security of personal data relating to pupils, parents, employees, contractors, and all members of the school community. The School recognises that responsible management of personal data is essential to maintaining trust, safeguarding children, and ensuring compliance with applicable legal and regulatory obligations.

This policy establishes the School's approach to:

- compliance with Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR),
- Czech data protection legislation and educational regulations,
- safeguarding the confidentiality and welfare of children,
- secure handling of educational, safeguarding, and employment records,
- responsible and secure use of information systems, digital platforms, and technology.

The School acknowledges that children's personal data requires enhanced protection, particularly within the Early Years Foundation Stage (EYFS) and Primary School environments, where sensitive educational, medical, behavioural, and safeguarding information may be processed.
The purpose of this policy is to:

- ensure personal data is processed lawfully, fairly, transparently, and securely,
- protect the rights and freedoms of pupils, parents, employees, and members of the school community,
- establish clear responsibilities for staff and third parties handling personal data,
- minimise the risks of unauthorised access, misuse, disclosure, loss, or data breaches,
- support the School's safeguarding, governance, cybersecurity, and operational responsibilities.

This policy applies to all personal data processed by the School in both electronic and paper formats and forms part of the School's wider safeguarding and compliance framework.

Aim

The aim of this GDPR & Data Protection Policy is to ensure that PORG International School processes all personal data responsibly, lawfully, securely, and in accordance with applicable data protection legislation and safeguarding obligations.

The School aims to:

- protect the privacy, dignity, and rights of pupils, parents, employees, and members of the school community,
- ensure compliance with Regulation (EU) 2016/679 (GDPR), Czech data protection legislation, and relevant educational requirements,
- establish a culture of confidentiality, accountability, and responsible data handling across the School,
- safeguard children's personal information, particularly within EYFS and Primary School environments,
- ensure that personal data is collected, used, stored, shared, retained, and disposed of securely and appropriately,
- minimise risks associated with unauthorised access, misuse, disclosure, cyber threats, or data breaches,
- ensure that all staff, contractors, and third parties understand their responsibilities regarding data protection and confidentiality,
- support effective safeguarding, educational, administrative, and operational processes while maintaining the highest standards of information security,
- promote transparency and trust between the School, pupils, parents, employees, and the wider community.

Through this policy, the School seeks to maintain a secure and compliant environment in which personal data is protected and handled with professionalism, care, and integrity at all times.

Legal Framework

This policy is based on:
• Regulation (EU) 2016/679 (General Data Protection Regulation),
• Czech Act No. 110/2019 Coll., on Personal Data Processing,
• Czech Education Act,
• safeguarding and child protection obligations,
• employment and labour legislation.

The School shall process personal data lawfully, fairly, transparently, and securely.

Scope

This policy applies to:
• employees,
• teachers,
• EYFS practitioners,
• contractors,
• volunteers,
• governors,
• consultants,
• third-party service providers processing school data.

It applies to all personal data processed by the School in paper or electronic form.

Definition

Personal Data

Any information relating to an identified or identifiable natural person ("data subject"). An identifiable person is one who can be identified directly or indirectly, particularly by reference to an identifier such as:

- name,
- identification number,
- location data,
- online identifier,
- photograph,
- pupil number,
- contact details,
- or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that individual.

Examples within the School environment include pupil records, parent contact information, staff employment records, attendance data, assessment results, CCTV footage, and digital communications.

Special Category Data

Personal data requires enhanced protection due to its sensitive nature. This includes information relating to:

- health and medical conditions,
- safeguarding and child protection records,
- Special Educational Needs (SEN),
- racial or ethnic origin,
- religious or philosophical beliefs,
- biometric data where applicable,
- psychological or behavioural information,
- disability-related information.

The School recognises that special category data concerning children requires a particularly high level of confidentiality, security, and safeguarding.

Processing

Any operation or set of operations performed on personal data, whether by automated or manual means.

- Processing includes:
- collection,
- recording,
- organisation,
- structuring,
- storage,
- adaptation,
- retrieval,
- consultation,
- use,
- sharing,
- transmission,
- disclosure,
- restriction,
- archiving,
- deletion,
- destruction.

Processing applies to both electronic and paper-based records managed by the School.

Data Protection Principles

The School shall ensure personal data is:
• lawfully, fairly and transparently processed,
• collected for specified purposes,
• adequate and relevant,
• accurate and up to date,
• stored only as long as necessary,
• processed securely.

Types of Data Processes

The School may process:
• pupil data,
• parent and guardian data,
• employee data,
• visitor and contractor data, including safeguarding, SEN, attendance, assessment, payroll, and CCTV records.

Lawful Bases for Processing

PORG International School processes data under one or more lawful bases, including:
• legal obligation,
• performance of a contract,
• legitimate interests,
• safeguarding obligations,
• consent where required,
• protection of vital interests.

Children's Data

PORG International School recognises that children merit specific and enhanced protection regarding the processing of their personal data. As an educational institution working closely with children in the Early Years Foundation Stage (EYFS) and Primary School environments, the School acknowledges its responsibility to ensure that all information relating to pupils is handled in accordance with the highest standards of confidentiality, safeguarding, and security. The School processes children's personal data only where necessary for legitimate educational, safeguarding, pastoral, health, administrative, or legal purposes.

Particular care shall be taken when handling sensitive information relating to:

- safeguarding and child protection matters,
- Special Educational Needs (SEN),
- medical and health information,

- behavioural and welfare records,
- assessment and educational progress,
- photographs and video recordings,
- online learning platforms and digital systems,
- counselling or pastoral support information.
- Additional safeguards shall apply to all records relating to children, including:
- restricted access based on role and legitimate need,
- enhanced confidentiality obligations for staff,
- secure digital and physical storage,
- password-protected systems and controlled permissions,
- secure transfer and sharing procedures,
- retention and disposal controls,
- monitoring of third-party educational technology providers.

Staff, contractors, volunteers, and third parties must:

- access only the information necessary for the performance of their duties,
- maintain strict confidentiality at all times,
- avoid discussing pupil information in inappropriate settings, ensure documents and devices containing pupil information are securely protected, and immediately report any actual or suspected data breaches or safeguarding concerns.

The School shall ensure that any use of digital learning platforms, educational applications, cloud services, photographs, or online communication tools involving children complies with GDPR requirements, safeguarding obligations, and appropriate parental consent requirements where applicable.

The School further recognises that the unauthorised disclosure or misuse of children's personal data may create safeguarding risks and therefore treats all pupil-related information with the highest level of care, professionalism, and responsibility.

Data Sharing

PORG International School may share personal data with selected third parties where necessary to fulfil its educational, safeguarding, legal, operational, or regulatory responsibilities. The School is committed to ensuring that all sharing of personal data is carried out lawfully, securely, proportionately, and in accordance with GDPR and applicable Czech legislation.

Personal data may be shared with:

- educational authorities and regulatory bodies,
- safeguarding and child protection authorities,
- healthcare professionals and medical providers,
- examination and assessment bodies,

- Special Educational Needs (SEN) professionals,
- external educational support services,
- IT service providers and cloud-based educational platforms,
- legal advisors, auditors, and insurers,
- law enforcement agencies,
- courts and regulatory authorities where legally required.

Examples of data sharing may include:

- pupil assessment and attendance information,
- safeguarding or welfare concerns,
- medical or emergency information,
- SEN documentation,
- examination registrations and results,
- secure use of educational applications and online learning systems,
- employment and payroll information for staff.

The School shall ensure that personal data is shared only where:

- there is a valid lawful basis under GDPR,
- the sharing is necessary and proportionate,
- the recipient has a legitimate need to receive the information,
- safeguarding obligations require disclosure,
- the sharing complies with legal or regulatory obligations,
- appropriate confidentiality and security measures are in place.

Where third-party service providers process personal data on behalf of the School, the School shall ensure that:

- appropriate Data Processing Agreements are in place,
- providers demonstrate adequate GDPR compliance,
- personal data is processed only on documented instructions,
- appropriate technical and organisational security measures are implemented,
- data is not retained longer than necessary.

The School shall take reasonable steps to ensure that all data sharing is conducted securely, including:

- use of password-protected systems,
- encrypted communication methods where appropriate,
- restricted access controls,
- secure transfer protocols,
- confidentiality obligations for recipients.

Special care shall be taken when sharing information relating to:

- safeguarding and child protection,

- EYFS pupils,
- medical or health information,
- SEN records,
- behavioural or welfare concerns.

The School recognises that unauthorised or inappropriate disclosure of personal data may create significant privacy and safeguarding risks and therefore requires all staff to exercise professional judgement, confidentiality, and care when handling or sharing personal information.

International Data Transfer

PORG International School recognises that certain educational, administrative, technological, and operational activities may require the transfer of personal data outside the European Economic Area (EEA). The School is committed to ensuring that any international transfer of personal data is conducted lawfully, securely, and in full compliance with Regulation (EU) 2016/679 (GDPR).

International data transfers may occur in connection with:

- cloud-based educational platforms,
- online learning systems,
- school communication applications,
- IT hosting and support services,
- safeguarding or welfare support systems,
- international educational programmes,
- external consultants or service providers,
- software providers operating outside the EEA.

Where personal data is transferred outside the EEA, the School shall ensure that appropriate safeguards are implemented, including:

- transfer to countries recognised by the European Commission as providing an adequate level of data protection,
- use of Standard Contractual Clauses (SCCs) approved by the European Commission,
- implementation of appropriate contractual, technical, and organisational safeguards,
- compliance with GDPR international transfer requirements,
- assessment of the security and privacy standards of third-party providers.

The School shall take reasonable steps to ensure that:

- transferred data remains secure and confidential,
- access to personal data is restricted to authorised persons only,
- third-party providers process data solely for authorised purposes,

- transferred data is protected against unauthorised access, disclosure, loss, misuse, or alteration.

Particular care shall be taken where international transfers involve:

- children's personal data,
- safeguarding records,
- SEN information,
- medical or health-related information,
- behavioural or welfare records,
- photographs or digital learning content.

Before engaging third-party providers that may process or store data outside the EEA, the School shall:

- conduct appropriate due diligence,
- assess GDPR compliance arrangements,
- ensure contractual protections are in place,
- evaluate data security measures and cybersecurity standards.

The School recognises that international transfers may present increased privacy and safeguarding risks and therefore requires all staff and service providers to ensure that personal data transferred internationally is handled with the highest standards of care, confidentiality, and security.

Data Retention

PORG International School is committed to ensuring that personal data is retained only for as long as necessary to fulfil educational, safeguarding, legal, operational, and regulatory obligations. The School recognises that appropriate retention and secure disposal of personal data are essential components of effective data protection, safeguarding, and information governance.

The School shall maintain a formal Data Retention Schedule specifying retention periods for different categories of records, including:

- pupil educational records,
- safeguarding and child protection files,
- SEN documentation,
- medical and welfare records,
- attendance and behavioural records,
- staff employment and recruitment files,
- payroll and financial records,
- visitor logs,

- CCTV recordings,
- complaints and disciplinary records,
- governance and compliance documentation.

Retention periods shall be determined in accordance with:

- GDPR requirements,
- Czech legal and regulatory obligations,
- safeguarding and child protection guidance,
- employment legislation,
- educational recordkeeping requirements,
- operational and insurance considerations.

The School recognises that certain categories of information, particularly safeguarding and child protection records, may require extended retention periods due to legal, welfare, or safeguarding obligations relating to children.

Personal data shall not be retained indefinitely unless legally required or justified by safeguarding or regulatory obligations. Once retention periods expire, personal data shall be securely deleted, anonymised, archived, or destroyed in a manner that prevents unauthorised access, disclosure, recovery, or misuse.

Secure disposal methods may include:

- confidential shredding of paper records,
- secure deletion of electronic files,
- destruction of storage media,
- removal from backup systems where appropriate,
- certified disposal by approved service providers.

The School shall ensure that:

- access to retained records is restricted to authorised personnel,
- archived records remain secure and confidential,
- retention practices are periodically reviewed,
- obsolete or unnecessary data is identified and removed appropriately.

Staff must not retain personal data on personal devices, unauthorised storage systems, or informal records beyond approved retention periods.

The School recognises that inappropriate retention or disposal of personal data may create significant privacy, safeguarding, legal, and cybersecurity risks. All employees and third parties handling School data are therefore required to comply fully with the School’s retention and secure disposal procedures.

Information Security

PORG International School is committed to maintaining appropriate technical, organisational, and administrative security measures to protect personal data against unauthorised access, disclosure, alteration, loss, misuse, destruction, or cyber threats. The School recognises that strong information security practices are essential to safeguarding children, protecting confidential information, ensuring operational continuity, and maintaining compliance with GDPR and applicable Czech legislation.

The School shall implement proportionate and risk-based security controls appropriate to the nature, sensitivity, and volume of personal data processed, particularly in relation to:

- children's information,
- safeguarding records,
- SEN documentation,
- medical and welfare records,
- employee records,
- financial information,
- digital learning platforms and online systems.

Technical Security Measures

The School shall implement appropriate technical safeguards, including:

- password-protected systems and devices,
- strong password requirements,
- multi-factor authentication where appropriate,
- encryption of sensitive data and portable devices,
- secure cloud storage solutions,
- firewalls and network security protections,
- antivirus and anti-malware protection,
- regular software and security updates,
- secure backup and disaster recovery procedures,
- monitoring and logging of system access,
- restricted user permissions based on role and legitimate need,
- secure Wi-Fi and network access controls,
- protection against phishing, ransomware, and cyberattacks.

The School shall ensure that backup systems are:

- regularly tested,

- securely stored,
- protected against unauthorised access,
- capable of supporting operational recovery in the event of data loss or cybersecurity incidents.

Organisational Security Measures

The School shall implement organisational controls, including:

- confidentiality obligations for all staff and contractors,
- GDPR and cybersecurity awareness training,
- safeguarding-focused data handling procedures,
- clear desk and clear screen expectations,
- visitor and physical access controls,
- secure handling of paper records,
- controlled access to archives and storage areas,
- incident reporting procedures,
- secure document disposal arrangements.

All employees, contractors, volunteers, and third parties handling School information are required to:

- maintain confidentiality at all times,
- access only to the information necessary for their duties,
- use School systems responsibly,
- avoid sharing passwords or login credentials,
- securely store devices and documents,
- report security incidents, data breaches, or suspicious activity immediately.

Remote Working and Mobile Devices

Where staff access School systems remotely or use portable devices, additional safeguards shall apply, including:

- secure remote access methods,
- password protection and encryption,
- approved software and applications only,
- prohibition of unsecured public storage platforms,
- secure handling of printed materials outside School premises.

Personal devices used for School business must comply with School security requirements where authorised.

Physical Security

The School shall maintain physical security measures to protect information and systems, including:

- restricted access to offices and secure areas,
- locked filing cabinets and storage rooms,
- CCTV monitoring where appropriate,
- visitor sign-in procedures,
- secure disposal bins for confidential waste.

Data Breach and Cybersecurity Incident Management

The School shall maintain procedures for identifying, reporting, investigating, and responding to:

- personal data breaches,
- cybersecurity incidents,
- unauthorised access attempts,
- phishing attacks,
- loss or theft of devices,
- accidental disclosures.

All actual or suspected incidents must be reported immediately to the designated Data Protection Coordinator or School Leadership.
The School shall:

- investigate incidents promptly,
- mitigate risks and impacts,
- maintain records of incidents,
- notify the Czech Office for Personal Data Protection (ÚOOÚ) where legally required,
- notify affected individuals where necessary.

Third-Party Security

Where external providers process personal data on behalf of the School, the School shall ensure that:

- appropriate contractual safeguards are in place,
- providers demonstrate adequate GDPR compliance,
- security standards are regularly reviewed,
- access to School data is restricted and monitored.

Staff Awareness and Training

The School recognises that information security depends on staff awareness and responsible behaviour. Regular training shall therefore be provided covering:

- GDPR obligations,
- safeguarding confidentiality,
- cybersecurity awareness,
- phishing and social engineering risks,
- secure handling of children's data,
- incident and breach reporting procedures.

The School recognises that information security is an ongoing responsibility requiring continuous monitoring, review, and improvement to address evolving technological, safeguarding, and cybersecurity risks.

Use of Photography and Video

PORG International School recognises the educational, safeguarding, pastoral, and communication value of photography and video recordings within the school environment. At the same time, the School acknowledges its responsibility to protect the privacy, dignity, safety, and rights of children, parents, employees, and members of the school community.

The School may collect, use, store, and publish photographs, video recordings, and digital images for legitimate educational and operational purposes, including:

- supporting teaching and learning activities,
- documenting school events and educational projects,
- promoting pupil achievements,
- internal school communications,
- newsletters and school publications,
- safeguarding and security purposes,
- educational assessments and observations,
- online learning platforms,
- school marketing and admissions materials,
- social media and website content where authorised.

The School recognises that images and recordings involving children require enhanced protection, particularly within the Early Years Foundation Stage (EYFS) and Primary School settings.

Consent Requirements

Parental or guardian consent shall be obtained where required by GDPR, Czech legislation, or School procedures, particularly for:

- publication of photographs or videos on the School website,
- use in promotional or marketing materials,
- social media publication,
- external media use,
- third-party educational platforms where applicable.

The School shall maintain records of parental consent preferences and ensure that staff are aware of any restrictions relating to individual pupils.
Parents and guardians may withdraw consent for certain uses of photographs or video recordings at any time, subject to legal, safeguarding, or operational limitations.

Safeguarding Considerations

The School shall take reasonable steps to ensure that the use of photography and video does not compromise safeguarding or child protection obligations.
In particular:

- children shall not be identified inappropriately alongside sensitive personal information,
- images shall not be used in a manner that may place children at risk,
- safeguarding restrictions relating to specific pupils shall be strictly observed,
- staff shall exercise professional judgement when capturing or sharing images.

Particular care shall be taken in relation to:

- looked-after children,
- safeguarding cases,
- court-related restrictions,
- children subject to confidentiality or protection measures.

Appropriate Use by Staff

Staff, contractors, volunteers, and visitors must:

- use only authorised School devices or approved systems where required,
- avoid storing pupil photographs on personal devices unless expressly authorised,
- ensure secure storage and transfer of digital files,
- comply with confidentiality and safeguarding obligations,
- avoid sharing images through personal social media or unauthorised platforms.

Photography or video recording in sensitive areas such as toilets, changing areas, medical rooms, or safeguarding spaces is strictly prohibited except where legally authorised and operationally necessary.

Educational and Observation Use

Within EYFS and Primary settings, photographs and videos may be used to:

- support learning observations,
- document educational progress,
- support assessment and developmental records,
- communicate learning activities with parents,
- support safeguarding and welfare monitoring where appropriate.

Such materials shall be securely stored and accessible only to authorised individuals.

Security and CCTV

The School may also operate video recording systems and CCTV for:

- safeguarding,
- site security,
- health and safety,
- incident investigation,
- protection of pupils, staff, and visitors.

CCTV systems shall:

- comply with GDPR requirements,
- be proportionate and justified,
- display appropriate signage,
- restrict access to authorised personnel only,
- retain recordings only for approved retention periods.

Storage and Retention

Photographs and video recordings containing personal data shall be:

- securely stored,
- protected against unauthorised access,
- retained only as long as necessary,
- deleted or destroyed securely when no longer required.

The School shall periodically review stored media to ensure continued lawful use and compliance with retention requirements.

Third-Party Platforms and Publications

Where photographs or videos are shared with external providers, educational platforms, or media organisations, the School shall ensure:

- appropriate safeguards are in place,
- data sharing is lawful and proportionate,
- third parties comply with GDPR obligations,
- children's privacy and safeguarding rights remain protected.

The School recognises that inappropriate use or disclosure of photography and video materials may create privacy, reputational, and safeguarding risks. All members of the school community are therefore expected to use photographs and video recordings responsibly, respectfully, and in accordance with this policy.

CCTV

PORG International School may operate Closed-Circuit Television (CCTV) systems as part of its safeguarding, health and safety, security, and operational management responsibilities. The School recognises that CCTV systems can play an important role in protecting pupils, employees, visitors, property, and the wider school community while also supporting incident prevention and investigation.
The use of CCTV shall always be proportionate, justified, and compliant with:

- Regulation (EU) 2016/679 (GDPR),
- Czech data protection legislation,
- safeguarding and child protection obligations,
- applicable security and employment laws.

Purpose of CCTV Monitoring

CCTV systems may be used for:

- safeguarding and protection of children,
- maintaining a safe learning environment,
- site and building security,
- prevention and detection of crime,
- protection of School property,
- health and safety monitoring,
- investigation of accidents, incidents, misconduct, or safeguarding concerns,
- supporting emergency response procedures,
- managing access to School premises.

The School shall ensure that CCTV is not used excessively or in a manner that unnecessarily intrudes upon the privacy of pupils, employees, or visitors.

Scope and Location of CCTV

CCTV cameras may be installed in appropriate areas including:

- school entrances and exits,
- reception and visitor access points,
- corridors and common areas,
- external grounds and playgrounds,
- car parks,
- perimeter security areas.

CCTV shall not normally be installed in areas where individuals have a heightened expectation of privacy, including:

- toilets and changing rooms,
- medical treatment areas,
- counselling or safeguarding rooms,
- private staff welfare areas,
  unless legally justified and authorised under exceptional circumstances.

Transparency and Signage

The School shall ensure that:

- CCTV use is clearly communicated,
- appropriate signage is displayed in monitored areas,
- individuals are informed about the purpose of CCTV monitoring,
- privacy notices include information regarding CCTV processing.

The School shall maintain transparency regarding:

- the lawful basis for CCTV use,
- retention periods,
- access controls,
- rights of individuals relating to CCTV recordings.

Access and Confidentiality

Access to CCTV footage shall be strictly restricted to authorised personnel with a legitimate operational, safeguarding, security, or legal need.

Authorised persons may include:

- School Leadership,
- Designated Safeguarding Leads (DSLs),
- IT and security personnel,
- authorised investigators,
- law enforcement authorities where legally required.

Individuals accessing CCTV footage must:

- maintain confidentiality,
- use recordings only for authorised purposes,
- comply with GDPR and safeguarding obligations,
- avoid unauthorised copying, sharing, or disclosure.

Unauthorised access, disclosure, or misuse of CCTV footage may result in disciplinary action and legal consequences.

Retention and Storage

CCTV recordings shall be:

- securely stored,
- password-protected where appropriate,
- protected against unauthorised access,
- retained only for as long as necessary.

The School shall define CCTV retention periods within its Data Retention Schedule. Footage relating to incidents, safeguarding concerns, investigations, or legal proceedings may be retained longer where necessary.
When recordings are no longer required, they shall be securely deleted or destroyed.

Data Subject Rights

Individuals may exercise applicable GDPR rights relating to CCTV recordings, including:

- the right to request access to footage containing their personal data,
- the right to request restriction of processing where applicable,
- the right to raise concerns regarding unlawful processing.

Requests shall be assessed in accordance with GDPR requirements while balancing:

- safeguarding considerations,
- privacy rights of third parties,
- legal and operational obligations.

Sharing of CCTV Footage

CCTV recordings may be shared with:

- law enforcement authorities,
- safeguarding authorities,
- legal representatives,
- insurers,
- regulatory authorities,

where legally permitted, necessary, and proportionate.

The School shall ensure that any sharing of CCTV footage is:

- properly authorised,
- documented where appropriate,
- conducted securely and confidentially.

Security and Monitoring

The School shall implement appropriate technical and organisational measures to protect CCTV systems, including:

- restricted system access,
- secure storage infrastructure,
- password protection,
- monitoring of system usage,
- regular maintenance and security updates.

Safeguarding and Child Protection

The School recognises that CCTV systems may involve the processing of children's personal data and therefore requires enhanced safeguarding and confidentiality measures.
CCTV shall never replace appropriate supervision, safeguarding procedures, or professional responsibility toward children's welfare.

All staff responsible for CCTV management shall receive appropriate training regarding:

- GDPR compliance,
- confidentiality,
- safeguarding,
- secure handling of recordings,
- incident reporting procedures.

The School recognises that responsible and proportionate use of CCTV forms part of its wider commitment to maintaining a safe, secure, and compliant educational environment for all members of the school community.

Data Subject Rights

Individuals may exercise rights including:
• right of access,
• rectification,
• erasure where applicable,
• restriction of processing,
• objection,
• data portability where applicable.

Requests shall be handled within GDPR timeframes.

Data Breaches

PORG International School recognises that personal data breaches may create significant risks to the privacy, safety, rights, and freedoms of pupils, parents, employees, and members of the school community. The School is committed to ensuring that all actual, suspected, or potential personal data breaches are identified, reported, investigated, managed, and resolved promptly and effectively.
Any actual or suspected personal data breach must be reported immediately to the School's designated Data Protection Coordinator, School Leadership, or other authorised responsible person.
A personal data breach may include, but is not limited to:

- loss or theft of devices containing personal data,
- accidental disclosure of confidential information,
- unauthorised access to systems or records,
- cyberattacks or hacking incidents,
- phishing or ransomware attacks,
- sending personal data to incorrect recipients,
- unauthorised sharing of photographs or pupil information,
- loss of safeguarding or SEN records,
- destruction or corruption of data,
- unauthorised access to CCTV footage,
- misuse of school systems or accounts.

Immediate Response

Upon becoming aware of a breach or suspected breach, staff must:

- report the incident immediately,
- take reasonable steps to contain or minimise the breach where possible,
- preserve relevant evidence,
- avoid deleting or altering affected information,
- cooperate fully with any investigation.

Failure to report a known breach may constitute a disciplinary matter.

Investigation and Risk Assessment

The School shall promptly investigate all reported incidents to determine:

- the nature and scope of the breach,
- the categories and volume of personal data involved,
- whether children's or special category data is affected,
- the cause of the incident,
- the potential risks to individuals,
- whether safeguarding concerns arise,
- whether legal or regulatory notification is required.

Particular priority shall be given to breaches involving:

- children's personal data,
- safeguarding records,
- SEN information,
- medical or welfare information,
- staff employment records,
- financial or sensitive confidential information.

Notification Obligations

Where legally required, the School shall notify:

- the Czech Office for Personal Data Protection (ÚOOÚ),
- affected individuals,
- safeguarding authorities,
- law enforcement authorities, where appropriate.

Notifications shall be made within applicable GDPR timeframes, including the requirement to report certain breaches to the supervisory authority within 72 hours of becoming aware of the breach, where feasible.

The School shall ensure that notifications include:

- the nature of the breach,
- categories of affected data,
- likely consequences,
- actions taken or proposed,
- mitigation measures,
- contact details for further information.

Containment and Mitigation

The School shall take reasonable steps to:

- contain the breach,
- prevent further unauthorised access or disclosure,
- recover affected systems or data,
- minimise harm to affected individuals,
- strengthen security controls where necessary.

This may include:

- password resets,
- disabling accounts,
- isolating systems,
- recovering devices,
- engaging IT or cybersecurity specialists,
- revising procedures or training.

Record Keeping

The School shall maintain a secure breach register documenting:

- details of incidents,
- investigations,
- risk assessments,
- actions taken,
- notifications made,
- outcomes and lessons learned.

Records shall be retained in accordance with the School's Data Retention Schedule and GDPR obligations.

Staff Responsibilities and Training

All staff, contractors, volunteers, and third parties handling School data are responsible for:

- maintaining confidentiality,
- following security procedures,
- recognising potential breaches,
- reporting incidents immediately,
- participating in GDPR and cybersecurity training.

The School shall provide regular awareness training covering:

- breach identification,
- phishing and cyber risks,
- secure handling of children's data,
- incident escalation procedures,
- safeguarding-related confidentiality risks.

Safeguarding Considerations

The School recognises that personal data breaches involving children may create safeguarding, welfare, reputational, or psychological risks. Breaches affecting children's data shall therefore be treated with heightened urgency, confidentiality, and sensitivity.
The School is committed to continuous improvement of its information security, incident response, and data protection practices in order to minimise the risk and impact of personal data breaches.

Staff Responsibilities

All employees, contractors, volunteers, consultants, and third parties working on behalf of PORG International School share responsibility for protecting personal data and maintaining confidentiality. The School recognises that effective data protection and information security depend on the awareness, professionalism, and responsible conduct of all members of staff.
All staff are required to:

- comply with this GDPR & Data Protection Policy and related School procedures,
- process personal data lawfully, fairly, securely, and confidentially,
- protect the privacy and rights of pupils, parents, employees, and members of the school community,
- access only the personal data necessary for the performance of their duties,
- use School systems, devices, networks, and digital platforms responsibly and securely,

- maintain confidentiality regarding safeguarding, SEN, medical, behavioural, and employment information,
- immediately report any actual or suspected data breach, cybersecurity incident, or unauthorised disclosure,
- follow secure storage, transfer, retention, and disposal procedures,
- protect passwords, login credentials, and access devices,
- avoid sharing confidential information through unauthorised channels or personal accounts,
- ensure that printed documents and portable devices are securely protected,
- comply with safeguarding obligations when handling children's information,
- participate in mandatory GDPR, safeguarding, cybersecurity, and information security training.

Confidentiality Obligations

Staff must maintain strict confidentiality regarding all personal and sensitive information obtained during the course of their work. Confidential information must not be:

- discussed in inappropriate or public settings,
- disclosed to unauthorised individuals,
- accessed for personal reasons,
- shared through insecure communication methods,
- retained unnecessarily.

Particular care must be taken when handling:

- safeguarding and child protection records,
- SEN documentation,
- medical and welfare information,
- behavioural and disciplinary records,
- staff employment information,
- photographs and video recordings of children.

Use of School Systems and Technology

All staff must use School technology and information systems responsibly, professionally, and securely. This includes:

- using only authorised systems and applications,
- following password and security requirements,
- locking devices when unattended,
- avoiding the installation of unauthorised software,
- complying with remote working and mobile device procedures,
- reporting suspicious emails, phishing attempts, or cybersecurity concerns immediately.

The use of personal devices for School business shall only be permitted where authorised and subject to School security requirements.

Training and Awareness

The School shall provide regular training and guidance covering:

- GDPR and data protection obligations,
- safeguarding confidentiality,
- cybersecurity awareness,
- phishing and cyber risks,
- secure handling of children's data,
- breach and incident reporting procedures,
- acceptable use of technology.

Staff are expected to actively engage with training and apply good data protection practices at all times.

Reporting Responsibilities

All staff have a duty to report:

- actual or suspected data breaches,
- loss or theft of devices or documents,
- unauthorised access to information,
- safeguarding concerns involving personal data,
- cybersecurity incidents,
- breaches of this policy.

Reports must be made immediately to the designated Data Protection Coordinator, School Leadership, or appropriate safeguarding lead.

Non-Compliance

Failure to comply with this policy, GDPR obligations, safeguarding confidentiality requirements, or School information security procedures may result in:

- disciplinary action,
- restriction of system access,
- contractual consequences,
- referral to regulatory authorities,
- legal action where appropriate.

The School recognises that maintaining high standards of confidentiality, safeguarding, and information security is essential to protecting children, maintaining trust, and ensuring a safe and compliant educational environment for the entire school community.

Data Protection Governance

PORG International School is committed to maintaining effective governance arrangements to ensure compliance with GDPR, Czech data protection legislation, safeguarding obligations, and recognised educational standards.

The School shall:

- monitor compliance with data protection requirements,
- maintain appropriate records of processing activities,
- implement and review data protection procedures,
- identify and manage risks relating to personal data,
- conduct audits and compliance reviews where appropriate,
- ensure appropriate staff training and awareness,
- review this policy and related procedures annually or following significant legal, operational, or safeguarding changes.

School Leadership shall oversee the implementation of this policy and ensure that appropriate technical and organisational measures are in place to protect personal data and maintain confidentiality.

The School is committed to continuous improvement of its data protection, safeguarding, and information security practices to ensure that personal data is handled responsibly, securely, and in accordance with applicable legal requirements.

Complaints

PORG International School is committed to handling concerns and complaints relating to personal data fairly, promptly, confidentially, and in accordance with GDPR and applicable Czech legislation.

Any individual who believes that their personal data has been processed improperly, unlawfully, insecurely, or in breach of this policy may raise a concern or complaint through the School's formal complaints procedure.

Complaints may relate to issues including:

- unauthorised disclosure of personal data,

- inaccurate or outdated information,
- inappropriate access to confidential records,
- misuse of photographs or video recordings,
- concerns regarding safeguarding confidentiality,
- failure to comply with GDPR rights,
- excessive retention of personal data,
- cybersecurity or data breach concerns,
- inappropriate sharing of personal information.

Complaints should normally be submitted in writing to the School's designated Data Protection Coordinator or School Leadership and should include sufficient detail to allow the concern to be properly investigated.

Upon receipt of a complaint, the School shall:

- acknowledge the complaint within a reasonable timeframe,
- investigate the matter appropriately and confidentially,
- review relevant records and circumstances,
- take corrective action where necessary,
- provide a response in accordance with applicable procedures and legal requirements.

The School shall handle complaints sensitively, particularly where they involve:

- children's personal data,
- safeguarding matters,
- SEN records,
- medical or welfare information,
- staff confidentiality concerns.

Individuals also have the right to raise concerns directly with the Czech supervisory authority for data protection:

Office for Personal Data Protection
(Úřad pro ochranu osobních údajů – ÚOOÚ)

The School encourages individuals to raise concerns internally in the first instance where appropriate so that issues may be addressed promptly and effectively. However, this does not affect the right of any individual to contact the supervisory authority or seek legal remedies under applicable data protection legislation.

Policy Review and Publication

This Policy is reviewed and updated annually and is published to all staff and volunteers. The PORG International School GDPR & Data Protection Policy is available to school personnel, teaching and non-teaching staff, pupils, and parents through the School information system.

Key Contacts

DSL	Thabang Lehner	lehner@porg.cz
Data Protection Officer	Michaela Comova	hotline@cca.cz
Principal	Barbora Gazdova	gazdova@porg.cz
Proprietor	Dagmar Dluhosova	dluhosova@prog.cz