Data Protection Policy
ISP School

Approved by:	**Governing Body**	**Date:** September 2024
Last reviewed on:	September 2024	
Next review due by:	September 2025	

ISP School – Data Protection Policy

CONTENTS

ISP School – Data Protection Policy

1. Introduction

ISP Schools process a high volume of personal data relating to workforce, pupils, parents/people with parental control, governors, visitors and other connected individuals (collectively known as data subjects). ISP Schools have a legal duty under data protection law to ensure the privacy of all data subjects by ensuring that all personal data is protected against unauthorised or unlawful processing and against accidental disclosure, loss, destruction or damage.

This policy sets out ISP Schools commitment to achieving good practice in the safe management of data processing in order to minimise potential breaches of information and ensure that all personal and sensitive information held is collected, processed, transferred, stored and disposed is in accordance with data protection law.

ISP School only collects personal data for specified, explicit and legitimate reasons. These reasons are covered in the ISP Privacy Notice, Workforce Privacy Policy and School Privacy Policy which are published and linked on the ISP School website.

2. Legislation and Guidance

This policy meets the requirements of the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). It is based on guidance published by the Information Commissioner's Office (ICO) and the ICO's code of practice for subject access requests.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Personal Data - is any information that relates to a living person who can be directly or indirectly identified from that information. This can include name, address, date of birth, an identification number, online identifier (eg. username) or anything specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person. It also includes any expression of opinion about that person. UK GDPR does not include anonymised data ie. where all identifying particulars have been removed and you cannot be personally identified.

Special Category Data - is a type of personal data which is more sensitive than other personal data and which therefore requires additional protection. Special category data includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics or biometric data, health (physical or mental), sex life and sexual orientation, criminal convictions and offences.

NB/ personal and special category data are collectively referred to as "personal data" in the rest of this document unless specified otherwise.

Processing - means the collection, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying of personal data. Processing can be automated or manual.

Data Controller - a person or organisation who (either alone or jointly with another person/organisation) determines the purposes and manner in which any personal data is processed.

Data Processor - a person or organisation who processes personal data on behalf and instruction of

the Data Controller.

Data Breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

ISP school acts as the Data Controller in terms of the records they process and the responsibility is delegated to the Director of Education.

The school is registered under ISP as a data controller with the Information Commissioner's Office and membership is renewed annually.

5. Roles and Responsibilities

Overview

This policy applies to all individuals employed by ISP school and to external organisations or individuals who process personal data for or on behalf of ISP School. This includes the workforce (i.e. employees, casual workers, agency workers, independent workers and contractors), stakeholders (governors) as well as external third parties (e.g. suppliers such as auditors, insurers and training providers).

Every individual who completes work for ISP School is responsible for the information they collect and process and accordingly could be held responsible for any breach or misuse of data. Where any suspected breach of this data protection policy occurs, the matter is to be reported to the Head Teacher, or the Deputy Head Teacher, in the Head Teacher's absence as a matter of urgency, who will then discuss with the Director of Education. The matter will be risk assessed and the actions taken which are proportionate to the breach or suspected breach. These actions will be reported to the Governing Body and the Data Protection Officer as soon as practicable, and certainly within 24 hours. All individuals should be aware that non-compliance with this policy could result in disciplinary action.

Governing Body

The Governing Body has overall responsibility for ensuring that ISP school complies with all relevant data protection obligations, including data quality, records management, ensuring compliance with all relevant legislation and privacy laws, risk management, incident management and information assets. Whilst responsibilities can be delegated, accountability cannot be delegated and that remains with the CEO of ISP.

Head Teacher

Day-to day responsibilities rest with the Head Teacher, or the Deputy Head Teacher in the Head Teacher's absence.

The Head Teacher has an extremely important role for ensuring and promoting good practice in the safe management of personal information. They are responsible for the implementation of this policy and ensuring compliance with data protection principles within their teams. They will: support incident investigations; ensure subject access requests and data breaches are addressed and recorded promptly and correctly; identify and address any training or additional training needs within their teams; report any incidents of non-compliance to the Governing Body; ensure all access rights for theirs teams are correct and closed swiftly when any individual leaves; ensure that data protection is routinely discussed at team meetings in order to raise awareness of responsibilities which allows for questions and support.

Data Protection Officer

ISP has an appointed Data Protection Officer (DPO) who can be contacted at DPO@polariscommunity.co.uk. The DPO is responsible for advising on all elements of this policy; monitoring and maintaining compliance with Data Protection Law and appropriate data protection registers and ICO memberships; championing privacy best practice; ensuring all staff are trained and aware of their responsibilities; developing related polices and guidelines to safeguard and mitigate any risks to the rights and interests of data subjects.

The DPO also provides advice and guidance on actions and responses for subject access requests, data breaches and Data Protection Impact Assessments (DPIA). They are also the point of contact for individuals about issues relating to the processing of personal information and for the Information Commissioners Office (ICO). The DPO is responsible for the timely reporting of any notifiable data breaches to the ICO that meet relevant thresholds under the UK GDPR.

Workforce and Connected Individuals

Every individual responsible for using personal data has a responsibility under UK GDPR to ensure it is collected and processed fairly and lawfully. Any individual who completes work for or on behalf of ISP School must do so in accordance with this Policy and must only access and process personal information that is relevant for them to perform their assigned roles and duties. Other responsibilities and obligations include:

- Raising any concerns with the Head Teacher if they become aware that this policy is not being followed
- Informing ISP of any changes to personal data
- Reading and understanding any policies and procedures relevant to their role
- Reporting any data breaches swiftly
- Complete all relevant mandatory training promptly or raise if additional training or support is needed to understand their responsibilities under UK GDPR

6. Data Protection Principles

All personal information will be processed in accordance with the six 'Data Protection Principles'. Personal data must be:

1. Processed lawfully and fairly
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and not excessive
4. Accurate and kept up -to-date
5. Kept for no longer than is necessary
6. Processed in a secure manner
7. Accountability

7. Data Protection Principle 1: Lawfulness, Fairness and Transparency

Collecting Personal Information

ISP School will only processes personal information where the law permits it. This is known as **the legal basis for processing** and there are 6 lawful bases (legal reasons):

- **Consent –** the data subject has given specific consent to process their personal information, e.g. in the course of subscribing to ISP newsletters, completing surveys, signing-up to events

or creating an online account via our websites

- **Contract –** is necessary so that the school can fulfil a contract or relationship with the data subject, or they have asked us to take specific steps before entering into a contract
- **Legitimate Interest -** where we, or a third party, have a legitimate interest in processing the personal information. A legitimate interest is where the processing of personal information is necessary to pursue legal or commercial interests in a way which is reasonably expected as part of running a business, but which is not detrimental to the fundamental rights and freedoms of the data subject and would have a minimal impact on their privacy. ISP School will always consider the fairness of all data processing and will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.
- **Public Interest –** is necessary to carry out a task or exercise a duty in the public interest
- **Legal Obligation** – is necessary to comply with legal or regulatory obligations. This includes Independent School Standards, employment, social security and social protection law amongst other
- **Vital Interest** - processing is necessary in order to protect the vital interests of a data subject or another natural person and generally applies to matters of life and death

ISP School may process personal data for more than one lawful ground depending on the specific purpose for which we are using the information.

8. Data Protection Principle 2, 3 and 4: Specified, Relevant and Accurate

Processing Personal Information

Specified – ISP School only collects personal data for specified, explicit and legitimate reasons. These reasons are covered in the ISP Privacy Notice, Workforce Privacy Policy and School Privacy Policy which are published and linked on the ISP School website.

Workforce, stakeholders and third parties must only process personal data where it is necessary in order to administer their roles. When personal data is no longer needed they must ensure it is deleted or anonymised. This will be done in accordance with the statutory regulations and the ISP School retention schedule.

Relevant – ISP School only use personal data for the purposes for which it was collected, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use personal data for an unrelated purpose, we will notify the data subject and will explain the legal basis which allows us to do so or seek consent where necessary. There may be times, where required or permitted by law, that ISP School processes personal data without the data subject's knowledge or consent.

Accurate – ISP School will ensure that all personal information collected, processed and stored remains accurate and up-to-date. Information will be checked when it is collected and at regular intervals/auditing and will be corrected where appropriate

9. Data Protection Principle 5: Kept For No Longer Than Necessary

Data Retention

ISP School will not keep personal information for any longer than for the purpose for which it was collected and processed, and in accordance with applicable law and regulations. Retention periods vary depending on the nature and context of the personal information and are based on the following criteria:

- For as long as we have reasonable business needs, such as managing our relationship with the data subject, and will only be as long as necessary to fulfil the purposes we collected it for
- For as long as someone could bring a claim against us
- Retention periods in line with legal and regulatory requirements or guidance

Personal information that is no longer required will be disposed of securely in accordance with ISP processes. Where we use third parties to safely dispose of records on ISP' behalf we require these third parties to provide sufficient guarantees that it complies with Data Protection law

10. Data Protection Principle 6: Processed in a Secure Manner

Data Security

ISP School is committed to the effective security of its people, equipment, offices and information. It has security measures in place to keep personal data safe and prevent it from being accidently or unlawfully lost, used or accessed in an unauthorised or unlawful way, altered, disclosed or damaged. In addition, personal data (and other non-personal data) is protected by the cyber security measures put in place, and ISP is Cyber Essentials and Cyber Essentials Plus certified.

ISP School limits access to personal data to those employees, agents, contractors and other third parties who have a business need to know only. They will only process personal information on our instructions, and are subject data protection law and confidentiality.

ISP School requires all third party service providers and other entities within the organisation to respect the security of personal data. ISP School will only share personal information where it is allowed or required by law, where it is necessary to administer the relationships with data subjects or where we have a legitimate interest to do so. We do not allow third party service providers to use personal data for their own purposes and we only permit them to process personal data for specified purposes and in accordance with our instructions and agreements. Third parties we may share with include:

- **IT -** such as other companies in our group and other service providers who support our website, IT and system administration services and reporting activities.
- **Advisors -** such as professional advisers, including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services.
- **Authorities:** - such as HM Customs & Excise, regulators, police and government bodies, or to otherwise comply with the law and other authorities who require reporting of processing activities.
- **Partnering organisations -** who assist us to provide or improve our services (e.g. by analysing and modelling statistics/data).

When doing this ISP will only appoint suppliers or contractors which can provide sufficient guarantees that they comply with Data Protection Law and we establish data sharing agreements where needed.

ISP School may also, at times need to share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our children, service users or workforce.

ISP School expects all who undertake work on its behalf to use systems, equipment and data in an appropriate and responsible way and must observe the guidance and guidelines as detailed in the organisation's IT associated policies and procedures to ensure usage is appropriate, ethical and lawful.

- All paper based records and portable electronic devices such as laptops and hard drives, are to be kept in lockable areas when not in use

- Paper documents containing personal data must not be left unattended in any areas of the school at any time. Computers and laptops screens should be locked when not in use.
- Where personal data needs to be taken off-site, this must be signed in and out from with the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment
- Encryption software is used to protect all electronic devices. USB devices are a security risk therefore there are restrictions on certain devices such as un-encrypted USB flash drives, USB hard drives, memory cards. However specific hardware encrypted USB drives are allowed and are provided by IT with authorisation. In exceptional circumstances access to other USB devices may be allowed if there is a particular business need, which IT will authorise.
- Corporate email should only be used for work purposes and not for personal use.
- When sending emails **'Check Twice, Send Once'** to ensure you are sending to the correct recipient. Also double check any attachments to the email.

11. Data Protection Principle 7: Accountability

UK GDPR requires organisations to put in place appropriate technical and organisational measures to demonstrate compliance with data protection law. ISP:

- Has appointed a Data Protection Officer
- Has produced clear, comprehensive data protection and data security policies and procedures
- Has a Privacy Notice and Privacy Policy which explains to data subjects how Polaris will process and protect their personal data
- Has implemented appropriate cyber and IT security measures and maintains external Cyber accreditations
- Conducts reviews and audits to test privacy measures and to ensure compliance
- Only process personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant Data Protection Law
- Ensures access to personal data is monitored and limited to those who have a business need to know only.
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to the rights and freedoms of individuals and when introducing new technologies
- Has written agreements, as appropriate, with external third parties who act in the capacities of Data Processors or Data Controllers and/or Joint Data Controllers
- Maintains records of processing activities
- Has a process for managing SAR and reporting data breaches
- Provides data protection training
- Uses retention schedules in line with applicable law and regulations

12. Data Subject Rights in Connection With Personal Information

Data protection law gives data subjects certain rights in respect of their personal data. Data subjects have the following rights:

- **Right to be informed** about the collection and processing of their personal information. This is covered in the Polaris Privacy Notice and specific service branded privacy policies which are published and linked on all the Polaris company websites.

- **Right to request access to your personal data** (commonly known as a "Subject Access Request). This enables data subjects to receive a copy of the personal data we hold about them and to check that we are lawfully processing it.

- **Right to request correction of the personal data** that we hold about them. This enables data subjects to have any incomplete or inaccurate data we hold corrected, however we may need to verify the accuracy of the new data provided.

- **Right to request erasure of the personal data** which enables data subjects to request deletion or removal of personal data where we no longer have a reason to process it or it is different to the purposes for which we originally collected it. However, we may not always be able to comply with this request of erasure dependent on specific legal or regulatory reasons.

- **Right to object to processing of the personal data** where we are relying on a legitimate interest (or those of a third party), and there is something about a data subject's particular situation which they believe impacts on their fundamental rights and freedoms. However this may be overridden where we can demonstrate we have compelling legitimate grounds to process the information which overrides their rights and freedoms. They also have the right to object where we are processing their personal data for direct marketing purposes.

- **Right to request restriction of processing of their personal data** which enables data subject's to ask us to suspend the processing of their personal data in the following scenarios: (a) they want to establish the data's accuracy; (b) where the use of the data is unlawful but they do not want us to erase it; (c) where they need us to hold the data even if we no longer require it as they need it to establish, exercise or defend legal claims; or (d) they have objected to our use of the data but we need to verify whether we have overriding legitimate grounds to use it.

- **Right to request the transfer of your personal data** which enables the data subject or their nominated third party to receive personal data that they have provided to us in a structured, commonly used and machine readable format.

- **Rights related to automated decision making including profiling** which enables the data subject to object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement) that might negatively affect them). However Polaris does not envisage that any decisions relating to individuals will be made via automated decision-making, including profiling.

All requests should normally be actioned within one calendar month. However, in exceptional circumstances this could be extended for up to a further two months and should be discussed with the Data Protection Officer.

Some of these rights are not absolute and therefore will not automatically apply when a data subject seeks to exercise their rights. ISP School will give written reasons it they believe that any given right does not apply.

Any request received should be forwarded to the Head Teacher/Deputy Head without delay to process and action.

13. Subject Access Requests (SAR)

Disclosure of curricular and educational records

Under the Data Protection Act 1998, every individual or their authorised representative has the right to obtain a copy of all their personal information and records held by an organisation. This is known as a

Subject Access Request (SAR) and helps individuals understand how and why organisations are using their data and check that it is being done lawfully.

A SAR can be submitted in any format, but we may be able to respond to requests more easily if they are made in writing and include:

- Name of the individual
- Correspondence address
- Contact number and email address
- Details of the information requested

All SARs should be forwarded to the Head Teacher as soon as possible to process and action. All SARs must be discharged within one calendar month of receipt.

NB/ refer to Subject Access Request Policy and Subject Access Request Procedure for guidance on processing a SAR.

Guidance for the data subject

When responding to a SAR we:

- May ask for some formal identification
- May contact you via phone to confirm the request was made
- Will respond to the SAR within one calendar month of receipt of your request (or receipt of any additional information needed to confirm your identity or clarity of your request)
- May request an extension of up to 3 months from receipt of your request, if the request is complex or multiple requests have been received. We will inform you of this within one month and explain why the extension is necessary
- If your request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision
- If we refuse a request, we will tell you why and that you have the right to complain to the Information Commissioners Office (ICO) or can seek to enforce your request through the courts.

We may not disclose certain information for a variety of reasons:

- You are only entitled to the personal information that relates to you. Any data that is the personal information of another individual and directly relates to that individual cannot be shared
- Providing the information might cause serious harm to your physical, emotional or mental health or condition or another individual
- Where records contain child abuse data (is being, has been or at risk of abuse) and disclosure would not be in the child's best interest
- Would include another individual's personal data that we cannot reasonably anonymise and we do not have the other individuals consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references or exam scripts

14. Request From a Child or on Behalf of a Child/Young Person by Someone with Parental Rights/Responsibilities

A child's personal data belongs to them and not to any third party, for example a parent or guardian. This applies even if the child is too young to understand the data subject access process. The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most requests from parents of pupils at our school may not be granted without the express permission of the pupil.

Before responding to any request for access to information held about a child, it will be considered whether the child is mature enough to understand their rights. If they are, they should be responded to rather than the parent. The following needs to be taken into account:

- The child's level of maturity and ability to make such decisions;
- The nature of the personal data;
- Any court orders relating to parental responsibility that may apply;
- Any duty of confidence and the possible consequences of allowing those with parental responsibility access to the child's information. This is particularly important if there have been allegations of abuse;
- Any detriment to the child if people with parental responsibility cannot access this information;
- The child's views on whether their parents/person with parental rights should have access to information about them

NB: In Scotland there is a presumption that a child aged 12 years or more has the capacity to make a subject access request. This does not apply in England, Wales or Northern Ireland,but it does indicate an approach that will be reasonable in many cases.

15. Parental Requests To View A Child's Educational Record

Under Regulation 5 of the Education (Pupil Information) (England) Regulations 2005 a parent is entitled to inspect their child's education record, free of charge within fifteen school days of receipt of the parent's written request for access to that record. Requests for a copy of all or part of a child's education record will be provided within fifteen school days of receipt of the parent's written request for access to that record and a charge maybe applicable.

As with a SAR (see above) an educational record belongs to that child, and not the child's parents. Therefore parents of pupils at this school do not have an automatic right to access their child's educational record. The school will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from the Information Commissioner's Office.

16. Personal Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. This includes breaches that are the result of both accidental and deliberate cause.

Examples of personal breaches can include:

- Sending personal data to an incorrect recipient or non-anonymised
- Computer devices containing personal data being lost or stolen
- Alteration of personal data

- Access by an unauthorised third party
- Loss of availability of personal data (e.g. when it has been encrypted by ransomware or accidently lost or destroyed)

ISP School will make all reasonable endeavours to reduce personal data breaches by minimising risks through good working practices as outlined in this Policy. In the event of a suspected data breach, the following steps should be taken:

- A soon as you suspect a breach of data protection has occurred immediately try to resolve/ reduce the impact of the breach eg. recall the email if it has been sent to an incorrect recipient, phone the recipient and ask them to delete etc.
- You must notify the Head Teacher or the Deputy Head Teacher, in the Head Teacher's absence as a matter of urgency, who will then discuss with the Director of Education. The matter will be risk assessed and actions taken which are proportionate to the breach or suspected breach. These actions will be reported to the Governing Body and the Data Protection Officer as soon as practicable, and certainly within 24 hours. The details must also be recorded on the Incident Portal if it reaches the threshold to report.

If there is a significant risk to people's rights and freedoms, the breach must be reported to the ICO without undue delay but not later than 72 hours after becoming aware of it. Failure to report within 72 hours must be explained to the ICO, and could result in a non-compliance and/or significant financial penalty. Reporting to the ICO is the responsibility of the DPO but in their absence will be Director of Education

Reporting a data breach as soon as it occurs will enable the correct advice to be given and appropriate action to be taken promptly. Effective management of such an incident can be vital in protecting ISP against financial, reputational and legal risks, and as such, it is essential that all those who discover a potential breach adhere to the following:

- Collect as many details about the incident as possible including the time, how the incident occurred, and who was involved, including the number of individuals and any contact details. Whilst exact details available will vary according to circumstance, ensure all possible details are collected as soon as possible
- Whilst collecting the above details, make a written note of any telephone calls received or discussions held about the incident, including the date and time of conversation
- Report the incident immediately to the Head Teacher and the Data Protection Officer
- The Data Protection Officer and the Head Teacher and/or Director of Education will agree a course of action and, if necessary, recommend that the Chief Executive Officer be informed
- Report the incident on the Incident Portal
- The severity of the incident will be assessed and, if necessary, a team will be identified who will be responsible for managing the incident. Precise membership may vary however a member of senior management will be required as the ultimate decision maker. The team must also have detailed knowledge as to any sector specific guidance as to the actions required in the event of a data protection breach.

The team will carry out the following:

- An investigation of the facts which will include the nature of the incident and the damage/harm that results or could result from the incident
- Take action to ensure a further breach does not occur and mitigate the harm caused as a result and/or any harm that may continue to result from the incident
- Consider which parties need to be notified of the incident. If there is a risk to people's rights and freedoms and it meet's the threshold for reporting, then the Information Commissioner's Office (ICO) will need to be notified. Consideration should also be given as to whether or not a third party may notify the ICO of the incident

- Other parties that need to be informed may include the individual(s) whose information was disclosed and ISP insurers
- If the Data Controller is identified as a Polaris customer, the contract for services will be checked in order to safeguard against any potential claim for liability.
- An investigation into any individual(s) who caused the incident may need to be carried out in conjunction with HR to decide whether or not disciplinary action is appropriate and to ascertain whether levels of training and guidance given were adequate or further is needed.
- A full review as to whether or not appropriate policies and procedures were in place and were followed, and whether any action needs to be taken in order to raise data protection and security compliance awareness.

17. CCTV

ISP School may use CCTV in various locations and sites to ensure they remain safe and for certain safeguarding purposes. ISP School will adhere to the ICO's code of practice for the use of CCTV to ensure that individual's rights and privacy are protected

ISP School does not need to ask an individual's permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by clear signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the Head Teacher.

CCTV footage is subject to UK GDPR in the same way as personal information and will be processed in line with this Data Protection Policy.

18. Photographs and Video

As part of our school activities, we may take photographs and record images of individuals within our school from time to time. Where this happens we will obtain written consent from all necessary individuals eg. parents/those with parental responsibility, pupils aged 18 years and over and we will clearly explain how the images will be used.

Photographs and videos taken by parents/those with parental responsibility at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parties have agreed to this.

Where our school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters etc
- Outside of school by external agencies such as school photographer, newspapers, campaigns
- Online on our school website or social media pages

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

19. Training

All staff and governors are provided with data protection training as part of their induction process to ensure they are able to demonstrate competence in their understanding of relevant legislation and best practice. Data protection training is available via Learnative and is mandatory for all staff, as well as those who complete work on behalf of ISP School and should be monitored via the supervisory process.

Data protection also forms part of continuing professional development and refresher training, where changes to legislation, guidance or the organisation's processes make it necessary. Records of all training activities are held with Human Resources.

20. Data Protection by Design and Default / Data Protection Impact Assessments

Data Protection by Design and Default is a legal requirement to ensure that we have considered data protection and privacy issues into all of our processing activities and business practices from the design stage of any system, service or process, at every stage of planning and then throughout the lifecycle.

Article 25(3) of the Data Protection Act 2018
'The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed'

Our change process is documented in the Polaris Group Business Management System ISO 9001:2015 and includes the requirement to identify changes that involve personal data and to ensure appropriate controls are in place.

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project and must be completed for any processing that is **likely to result in a high risk** to the rights and freedoms of individuals. A DPIA must:

- describe the nature, scope, context and purposes of the processing
- assess necessity, proportionality and compliance measures
- identify and assess risks to individuals
- identify any additional measures to mitigate those risks

21. Compliance/Monitoring

The Polaris Board and Senior Leadership Team have ultimate responsibility for ensuring that the organisation complies with all business and UK GDPR obligations. Every individual who completes work on behalf of ISP will abide by this Data Protection Policy and other relevant security procedures to ensure any personal data they process is protected.

The Data Protection Officer will monitor and review compliance with this policy and is a member of the Polaris risk management team. The risk management team meet monthly, and this informs compliance to the Senior Leadership Team and ultimately to the Polaris Board. Information reported can cover:

- Details of subject access requests
- Details of the exercise of other individual rights
- Completion/uptake of mandatory training on Learnative
- Breaches and the responses to each including ICO reporting
- Other contact with ICO
- Results of internal audits
- Results of cyber security testing

The Head Teacher, Director of Education and Governing Body are responsible for monitoring and reviewing this policy.

22. Transferring Personal Data Overseas

Polaris does not envisage that personal data will be transferred outside of the UK or the EU. However if at any time this was necessary this would be in line with UK Data Protection Law where the UK

government has decided the particular country or international organisation ensures an adequate level of protection of personal data (known as an 'Adequacy Decision').

23. Complaints About Data Processing

All data subjects have the right to make a complaint if they have concerns about how their personal information is being processed by Polaris. Complaints should be made directly to the manager of the relevant service brand in the first instance and will be handled in accordance with the Polaris complaints policies.

Should data subjects have concerns about how their complaint has been handled then they have the right to make a complaint directly to the Information Commissioner's Office (ICO) which is the UK supervisory authority for data protection issues (www.ico.org.uk).

Document Review History

Version Number	Review Date	Amendments/Updates
1 - Teynham School	July 2020	N/A
2 - Teynham	July 2021	N/A
3 - Teynham	July 2022	**OBSOLETE - New policy produced Nov 2023 to cover all ISP schools.(Teynham, Battle & Whitstable)**
1 - Battle	July & Sept 2023	**OBSOLETE - New policy produced Nov 2023 to cover all ISP schools (Teynham, Battle & Whitstable)** Completely re-written and removed CCTV as not relevant to our school and Information Commissioner's Office has removed its code of conduct for surveillance cameras Revisited Sept 2022 to bring review in line with other policies
1 – ISP Schools	Nov 2023	New policy produced to cover GDPR legislation and all ISP schools
2 – ISP Schools	Sept 2024	Annual review completed. No changes.