Data Protection Policy

Contents

1. Introduction - Why this policy matters at Waterside School 1
2. Legal framework and guidance 1
3. Definitions and shared understanding 2
4. The data controller 2
5. Roles and responsibilities 2
6. Data protection principles 3
7. Lawful, fair and transparent collection of data 3
8. Data minimisation, accuracy and retention 4
9. Sharing personal data 4
10. Rights of individuals and subject access requests 4
11. Learner and data rights 4
12. When information may be withheld 5
13. Educational records 5
14. CCTV 5
15. Photographs and videos 5
16. Artificial intelligence (AI) 5
17. Data protection by design and default 5
18. Data security and storage 6
19. Disposal of records 6
20. Data breaches 6
21. Training and complaints 6
Appendix 1 – Independent School Standards Mapping of Policy 6
Appendix 2 - Personal Data Breach Procedure 7
Actions to minimise the impact of data breaches 9

1. Introduction - Why this policy matters at Waterside School

Waterside School is a specialist SEND school supporting learners with Autism Spectrum Condition (ASC) and Social, Emotional and Mental Health (SEMH) needs. Many learners and families share highly sensitive personal information with us so that we can provide safe, appropriate and effective education and care. We recognise that information sharing is built on trust, and that trust is especially important for learner and families who may have experienced trauma or adversity.

This policy explains how Waterside School, collects, stores, uses and protects personal data lawfully, respectfully and transparently. It reflects our safeguarding duties, trauma-informed practice, and commitment to always acting in the best interests of learner. The policy applies to all personal data, regardless of whether it is held electronically, on paper, verbally, visually (including CCTV), or in any other form.

2. Legal framework and guidance

This policy complies with the UK General Data Protection Regulation (UK GDPR), which is incorporated into UK law through the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020, and with the Data Protection Act 2018. It is informed by guidance from the Information Commissioner's Office (ICO), including guidance on CCTV and personal information, and by Department for Education (DfE) guidance, including advice on the use of generative

artificial intelligence in education. These arrangements support compliance with the Independent School Standards and Ofsted expectations regarding leadership, governance, safeguarding and information management.

3. Definitions and shared understanding

Personal data means any information relating to an identified or identifiable living individual. This includes names, identification numbers, location data and online identifiers such as usernames. It also includes information relating to a person's physical, physiological, genetic, mental, economic, cultural or social identity.

Special category personal data is more sensitive and therefore requires a higher level of protection. This includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, physical or mental health, and a person's sex life or sexual orientation.
Processing refers to anything done with personal data, whether manually or electronically. This includes collecting, recording, organising, storing, adapting, retrieving, using, sharing, erasing or destroying data.

A data subject is the individual whose personal data is being processed. A data controller is the organisation that determines why and how personal data is processed, and a data processor is an organisation or individual that processes data on behalf of the controller. A personal data breach is any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Waterside School, processes personal data relating to learners, parents and carers, staff, governors, visitors and others, and therefore acts as a data controller. Waterside School is registered with the Information Commissioner's Office, as required by law.

5. Roles and responsibilities

This policy applies to all staff employed by Waterside School, as well as to external organisations or individuals working on our behalf. Failure to comply with this policy may result in disciplinary action.

The Governing Board has overall responsibility for ensuring that the school complies with data protection legislation. This forms part of its duties under the Independent School Standards relating to leadership, governance and safeguarding.

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidance where appropriate. The DPO provides an annual report to the Governing Board and advises on data protection risks and improvements. The DPO

is also the first point of contact for individuals whose data is processed and for the ICO. The school's DPO is Dani, who can be contacted at Insert Dani's Email Address.

The Headteacher acts as the day-to-day representative of the data controller and is responsible for ensuring that this policy is embedded in practice.

All staff are responsible for collecting, storing and processing personal data in accordance with this policy, keeping information secure, and informing the school of changes to their own personal data. Staff must contact the DPO if they have questions about data protection law, are unsure whether they have a lawful basis to use data, need to obtain consent or draft a privacy notice, are sharing data with third parties, are transferring data outside the UK, are engaging in new activities that may affect privacy rights, or become aware of a data breach.

6. Data protection principles

Under UK GDPR, personal data must be processed lawfully, fairly and transparently. It must be collected for specified, explicit and legitimate purposes, be adequate, relevant and limited to what is necessary, be accurate and kept up to date, be retained only for as long as necessary, and be processed in a way that ensures appropriate security. These principles underpin all data handling at Waterside School and align with trauma-informed practice by promoting predictability, fairness and trust.

7. Lawful, fair and transparent collection of data

Waterside School only processes personal data where there is a lawful basis under UK GDPR. These include processing necessary to fulfil a contract, comply with a legal obligation, protect vital interests such as safeguarding life, perform a task in the public interest or under official authority, pursue legitimate interests that do not override individual rights, or where clear and informed consent has been given.

Where special category personal data is processed, one of the additional legal conditions is also met. These include explicit consent, employment or social protection obligations, protection of vital interests where consent cannot be given, data made public by the individual, legal claims, substantial public interest, health or social care purposes, public health reasons, or archiving, research or statistical purposes in the public interest.

Criminal offence data is processed only where both a lawful basis and a specific legal condition apply, such as consent, safeguarding vital interests, legal proceedings or substantial public interest.

Whenever personal data is collected directly, individuals are provided with the information required by law through privacy notices. The school considers fairness carefully and ensures that data is not used in ways that individuals would not reasonably expect or that could cause unjustified harm.

8. Data minimisation, accuracy and retention

Personal data is collected only for clear, explicit and legitimate purposes, which are explained at the point of collection. If data is required for a new purpose, individuals are informed and consent is sought where necessary. Staff access and process only the data necessary to carry out their roles. Data is kept accurate and up to date, and inaccurate or unnecessary data is rectified, erased, deleted or anonymised appropriately. Data is retained only for as long as necessary and in line with retention schedules.

9. Sharing personal data

Waterside School does not normally share personal data without consent. However, sharing may be necessary where there is a risk to staff safety, where the school needs to work with other agencies in a learner's best interests, or where suppliers or contractors require data to provide services. In such cases, the school ensures that third parties comply with UK data protection law, that appropriate contracts are in place, and that only necessary data is shared.

Personal data may also be shared with law enforcement agencies, government bodies, emergency services or local authorities where legally required or to respond to emergencies. Any international transfers of personal data are carried out in accordance with UK data protection law.

10. Rights of individuals and subject access requests

Individuals have the right to make a subject access request to access personal data held about them. This includes confirmation that data is being processed, access to a copy, information about purposes, categories of data, recipients, retention periods, rights to rectification or erasure, the right to complain to the ICO, information about data sources, automated decision-making, and safeguards for international transfers. Requests may be made verbally or in writing. Staff must forward all requests immediately to the DPO. When responding, the school may request identification, verify requests by phone, and will respond within one month, free of charge. Extensions of up to three months may apply for complex or numerous requests.

11. Learner and data rights

Personal data belongs to the learner, not automatically to parents or carers. Parents may make a request on behalf of a learner only where the learner lacks capacity to understand their rights or has given consent. Learner aged 12 and above are generally presumed capable, but decisions are made on a case-by-case basis, considering SEND, communication needs and emotional wellbeing.

12. When information may be withheld

Information may be withheld where disclosure would cause serious physical or mental harm, reveal safeguarding concerns or abuse investigations, breach another person's privacy, or involve legally protected documents such as legal advice, confidential references or exam scripts. Unfounded or excessive requests may be refused or charged a reasonable administrative fee. Individuals are informed of their right to complain to the ICO.

13. Educational records

Parents or those with parental responsibility may request access to educational records. The school aims to respond within 15 school days of a written request and may charge a fee. Requests may be refused where disclosure would cause harm or release exam results prematurely.

14. CCTV

CCTV is used on site to support safeguarding and site security. The school follows ICO guidance, uses clear signage and restricts access to recordings. Enquiries should be directed to the Headteacher.

15. Photographs and videos

Written consent is obtained for photographs and videos of learners. The purpose of use is clearly explained, and consent can be withdrawn at any time. Images may be used internally, in approved media, or on the school's website or social media. Images are not accompanied by identifying information. Parents are asked not to share images of other learners online without consent. Further detail is contained in the Safeguarding Policy.

16. Artificial intelligence (AI)

AI tools may support learning but pose risks to personal data. Personal or sensitive data must not be entered into unauthorised AI tools. Any misuse is treated as a data breach and managed under the breach procedure.

17. Data protection by design and default

Data protection is embedded in all processing activities. The school appoints a qualified DPO, carries out data protection impact assessments where required, integrates data protection into policies and systems, trains staff regularly, audits practice, and maintains detailed records of processing activities.

18. Data security and storage

Personal data is protected against unauthorised access, loss or damage. Paper records and portable devices are securely stored, confidential papers are not left accessible, data taken off site is signed in and out, strong passwords are used, encryption protects portable devices, and personal devices are not used without permission. Due diligence is carried out when sharing data with third parties.

19. Disposal of records

Personal data that is no longer required or is inaccurate is securely destroyed. Paper records are shredded or incinerated, and electronic files are securely deleted. Third-party disposal services must comply with data protection law.

20. Data breaches

The school aims to prevent data breaches. Where a breach is suspected, the procedure in Appendix 1 is followed, including reporting to the ICO within 72 hours where required.

21. Training and complaints

All staff and governors receive data protection training at induction and through ongoing CPD. Complaints are handled by the Head Teacher in line with the Complaints Policy.

Appendix 1 – Independent School Standards Mapping of Policy

Independent School Standard	How this policy meets the standard
Part 3 – Welfare, Health & Safety	Secure handling of safeguarding and health data. CCTV oversight; breach management
Part 4 – Suitability of Staff	Secure storage and processing of staff records
Part 6 – Provision of Information	Transparency through privacy notices and SAR processes
Part 7 – Manner in which complaints are handled	Clear routes for complaints and ICO escalation
Part 8 – Leadership & Management	Governance oversight, DPO reporting, audits, training, compliance systems

Appendix 2 - Personal Data Breach Procedure

This personal data breach procedure is based on guidance issued by the Information Commissioner's Office (ICO) and applies to all staff, governors, volunteers, contractors and data processors working for or on behalf of Waterside School. The purpose of this procedure is to ensure that any personal data breach or suspected breach is identified, contained, investigated, reported and learned from in a timely, lawful and proportionate way, with regard to safeguarding, wellbeing and the rights of children and families.

Where a member of staff, governor or data processor discovers, causes or suspects a personal data breach or a potential breach, they must notify the Data Protection Officer (DPO) immediately by email. Prompt reporting is essential to reduce harm and to ensure that statutory timescales can be met. No attempt should be made by the individual to investigate the breach independently beyond taking immediate steps to prevent further loss where it is safe and appropriate to do so.

Upon receiving a report, the DPO will investigate the matter and determine whether a personal data breach has occurred or is likely to have occurred. In making this determination, the DPO will consider whether personal data has been accidentally or unlawfully lost, stolen, destroyed, altered, disclosed, made available where it should not have been, or accessed by unauthorised individuals. The DPO will take into account the nature of the data involved, including whether it includes special category or safeguarding information, and the context in which the incident occurred.

All staff and governors are expected to cooperate fully with the investigation. This may include providing information, answering questions and allowing access to relevant systems or records. Investigations under this procedure are not treated as disciplinary investigations, although separate processes may be considered later if appropriate.

If the DPO determines that a personal data breach has occurred, or that it is likely a breach has occurred, the DPO will inform the Headteacher and the Chair of Governors without delay. This ensures appropriate leadership oversight and enables safeguarding, operational and reputational risks to be managed at a senior level.

The DPO will take all reasonable steps to contain the breach and to minimise its impact. This may involve working with relevant staff members, external data processors or IT providers, and seeking specialist external advice where necessary. Actions will be proportionate to the nature and severity of the breach and informed by the specific risks to individuals. Reference will be made to the actions outlined later in this procedure for particular types of data breach.

The DPO will assess the potential consequences of the breach by considering both the seriousness of the possible harm and the likelihood of that harm occurring. This assessment will be carried out both before and after mitigation steps are implemented, to ensure that risks are reduced as far as reasonably possible.

Using the ICO's breach self-assessment tool, the DPO will decide whether the breach must be reported to the ICO and whether affected individuals must be informed. This

decision-making process is documented carefully, regardless of the outcome, to demonstrate accountability and compliance with data protection law. Records of decisions and actions taken are stored securely on Waterside School's computer system.

Where the breach meets the threshold for reporting to the ICO, the DPO will notify the ICO via the "report a breach" page on the ICO website or via the ICO breach report line on 0303 123 1113. This notification will be made within 72 hours of Waterside School becoming aware of the breach. The report will include, where possible, a description of the nature of the personal data breach, the categories and approximate number of individuals affected, the categories and approximate number of personal data records concerned, the name and contact details of the DPO, a description of the likely consequences of the breach, and a description of the measures that have been taken or will be taken to address the breach and mitigate adverse effects.

If not, all required information is available within 72 hours, the DPO will submit the information that is available within the statutory timeframe and will explain the reasons for the delay, along with an indication of when further information is expected. Any remaining information will be provided to the ICO as soon as it becomes available.

Where Waterside School is required to notify individuals whose personal data has been affected by a breach, the DPO will communicate with those individuals in writing. This communication will be clear, calm and written in plain language. It will explain the nature of the breach, provide the name and contact details of the DPO, describe the likely consequences of the breach, and outline the measures that have been taken or will be taken to address the breach and reduce any potential harm.

Following the investigation and any communication with affected individuals, the DPO will consider whether it is appropriate to notify relevant third parties who may be able to help mitigate potential harm. This may include, for example, the police, insurers, banks, credit card companies or safeguarding partners, depending on the nature of the breach.

Every personal data breach is documented by the DPO, regardless of whether it is reported to the ICO. For each breach, records will include the facts and cause of the breach, its effects, and the actions taken to contain it and to reduce the likelihood of recurrence. This may include changes to processes, systems or training.

All records of personal data breaches are stored securely on Waterside School's computer system. The DPO and the Headteacher will meet as soon as reasonably possible after a breach to review what happened and to agree actions to prevent a similar incident occurring again. In addition, the DPO and Headteacher will meet on a termly basis to review all recorded breaches, identify patterns or trends, and determine whether further action is required to reduce future risk.

Actions to minimise the impact of data breaches

The school recognises that some types of data breach carry higher risks, particularly where safeguarding or special category data is involved. The steps outlined below describe how the school would seek to mitigate harm in specific scenarios. The effectiveness of these actions will be reviewed after any breach and amended where necessary.

Where special category or sensitive information, including safeguarding records, is accidentally disclosed via email to unauthorised recipients, the sender must attempt to recall the email immediately upon becoming aware of the error. Any member of staff who receives personal data in error must notify both the sender and the DPO as soon as they become aware of the issue.

If the sender is unavailable or unable to recall the email, the DPO will contact the school's IT contractor, to attempt to recall the message from external recipients and to remove it from the school's email system. A copy may be retained where required for evidential purposes.

Where recall is unsuccessful or cannot be confirmed, the DPO will consider whether it is appropriate to contact the unauthorised recipients directly. In such cases, the DPO may explain that the information was sent in error and formally request that recipients delete the information and do not copy, share, save, publish or replicate it in any way. The DPO will seek written confirmation from recipients that they have complied with this request wherever possible.

The DPO will also conduct internet searches to check whether the information has been made public. If it has, the DPO will contact the relevant website owner, administrator or publisher to request removal and deletion of the information.

If safeguarding information is compromised, the DPO will inform the Designated Safeguarding Lead and will discuss whether local safeguarding partners should be notified, in line with statutory safeguarding duties and the best interests of the child.

Where a different type of data breach occurs, similar principles will be applied. Examples may include the publication of pupil premium intervention details for named children, the sharing of non-anonymised exam results or staff pay information with governors, the theft or hacking of a school laptop containing unencrypted sensitive data, or hard-copy reports being sent to the wrong pupils or families. In all cases, Waterside School will seek to recall the data, remove it promptly, understand the scale and reach of the breach, liaise with affected individuals and relevant authorities, and take appropriate follow-up action.