GDPR DATA PROTECTION POLICY

The Central Team and DPO will review this policy on a 2 yearly cycle

Policy Version:	V4
Colleagues affected by this Policy:	All stakeholders
Person responsible for the Policy:	Chief Operating Officer
Approved by/ date:	CEO/ Sept 2023
Next review:	Sept 2025

Contents:

Statement of intent

1. Legal framework
2. Applicable data
3. Principles
4. Accountability
5. Data protection officer (DPO)
6. Lawful processing
7. Consent
8. Disclosures of personal data
9. Limitation, minimisation and accuracy
10. The right to be informed
11. The right of access
12. The right to rectification
13. The right to erasure
14. The right to restrict processing
15. The right to data portability
16. The right to object
17. Privacy by design and privacy impact assessments
18. Data breaches
19. Data security
20. Publication of information
21. CCTV and photography
22. Data retention
23. DBS data
24. Training
25. Policy review

Appendix One – Special Category Data Policy

Statement of Intent

The Sea View Trust is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

The Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other Trusts and educational bodies, and potentially social services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Trust complies with the following core principles of the UK GDPR.

Organisational methods for keeping data secure are imperative, and The Sea View Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the UK GDPR and the DPA, which came into effect in May 2018.

Signed by:

_____ Executive Leader Date:

1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

· The General Data Protection Regulation (UK GDPR)

. The Data Protection Act 2018

· The Freedom of Information Act 2000

.

· The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

· The Trust Standards and Framework Act 1998

1.2. This policy will also have regard to the following guidance:

· Information Commissioner's Office UK GDPR Guidance and Resources

1.3. This policy will be implemented in conjunction with the following other Trust policies:

· Compliant Records Management Policy

· Data Breach Policy

· Surveillance and CCTV Policy

. Subject Access Request Procedure

2. Applicable data

2.1. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2.2. **Sensitive personal data** is referred to in the UK GDPR as **'special categories of personal data'**, which are **i**nformation revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

2.3 For the purposes of this policy, **data subject** means the individual whose personal data is held or processed.

2.4 For the purposes of this policy, **processing** refers to any operation performed on personal data such as collecting, recording, organising, structuring, storing, altering, retrieving, using, disseminating, erasing or destroying personal data.

3. Principles

3.1. In accordance with the requirements outlined in the UK GDPR, personal data will be:

. Processed lawfully, fairly and in a transparent manner in relation to individuals.

. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

. Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.

. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.2. The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4. Accountability

4.1. The Sea View Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.

4.2. The Trust will provide comprehensive, clear and transparent privacy policies.

4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

4.4. Internal records of processing activities will include the following:

· Name and details of the organisation

· Purpose(s) of the processing

· Description of the categories of individuals and personal data

· Retention schedules

· Categories of recipients of personal data

· Description of technical and organisational security measures

· Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

4.5. The Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:

· Data minimisation.

· Pseudonymisation.

· Transparency.

· Allowing individuals to monitor processing.

· Continuously creating and improving security features.

4.6. Data protection impact assessments will be used, where appropriate.

5. Data protection officer (DPO)

5.1. A DPO will be appointed in order to:

· Inform and advise the Trust and its employees about their obligations to comply with the UK GDPR and other data protection laws.

· Monitor the Trust's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

5.2. The DPO will report to the highest level of management at the Trust, which is the Executive Leader.

5.3. The DPO will operate independently and will not be penalised for performing their task.

5.4. Sufficient resources will be provided to the DPO to enable them to meet their UK GDPR obligations.

6. Lawful processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed.

6.2. Under the UK GDPR, data will be lawfully processed under the following conditions:

· The consent of the data subject has been obtained.

· Processing is necessary for:

— Compliance with a legal obligation.

— The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

— For the performance of a contract with the data subject or to take steps to enter into a contract.

— Protecting the vital interests of a data subject or another person.

— For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

6.3. Sensitive data will only be processed under the following conditions:

· Explicit consent of the data subject, unless reliance on consent is prohibited by UK law.

· Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

· Processing relates to personal data manifestly made public by the data subject.

· Processing is necessary for:

— Carrying out obligations under employment, social security or social protection law, or a collective agreement.

— Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.

— The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

— Reasons of substantial public interest on the basis of UK law which is proportionate to the aim pursued and which contains appropriate safeguards.

— The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of UK law or a contract with a health professional.

— Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

— Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1) UK GDPR.

6.4. Where the Trust processes sensitive data on the basis that it is for reasons of substantial public interest or for the purposes of employment, the Trust does so in accordance with its Special Category Data Policy which is set out at Annex One.

7. Consent

7.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

7.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.3. Where consent is given, a record will be kept documenting how and when consent was given.

7.4. The Trust ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

7.6. Consent can be withdrawn by the individual at any time.

7.7. The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child.

8. Disclosures of personal data

8.1 The Trust will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. The Trust will comply with data protection law when disclosing this information.

8.2 If the Trust becomes aware of a staff safety issue with regards to one of our pupils or parents/guardians, the Trust will share that information with the appropriate teams and/or individuals to ensure the safety of all concerned.

8.3 The Trust may share personal data in some circumstances with other agencies. The Trust will obtain the necessary consents before referring pupils to another agency where we are required to do so.

8.4 The Trust will share personal data with suppliers and/or contractors who enable the school to provide services to staff and pupils – e.g. IT companies or energy suppliers. The data shared is limited to the specific information the supplier requires in order to carry out their service as well as any additional information that ensures the Trust fulfils its health and safety obligations to the people carrying out the work. The Trust will ensure that suppliers handle this data correctly through the contract terms and will only use suppliers and/or contractors that comply with data protection law.

8.5 We will be responsible for the fair and lawful processing of personal data shared with third parties. We make sure this occurs through data sharing agreements, either in contracts or as standalone agreements.

9. Limitation, minimisation and accuracy

9.1 The Trust will only process personal data for specified, explicit and legitimate reasons. The school will explain these reasons to individuals when personal data is first collected.

9.2 If the Trust wants to use personal data for reasons other than those given when it is first obtained, the Trust will inform the individuals concerned and seek consent where necessary.

9.3 Staff must only process personal data where it is necessary to do their jobs.

10. The right to be informed

10.1. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

10.2. If services are offered directly to a child, the Trust will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

10.3. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

· The identity and contact details of the controller, and where applicable, the controller's representative and the DPO.

· The purpose of, and the legal basis for, processing the data.

· The legitimate interests of the controller or third party.

· Any recipient or categories of recipients of the personal data.

· Details of transfers to third countries and the safeguards in place.

· The retention period of criteria used to determine the retention period.

· The existence of the data subject's rights, including the right to:

— Withdraw consent at any time.

— Lodge a complaint with the Information Commissioner's Office.

· The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

10.4. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

10.5. Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

10.6. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

10.7. In relation to data that is not obtained directly from the data subject, this information will be supplied:

· Within one month of having obtained the data.

· If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

· If the data are used to communicate with the individual, at the latest, when the first communication takes place.

11. The right of access

11.1. Individuals have the right to obtain confirmation that their data is being processed.

11.2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

11.3. The Trust will verify the identity of the person making the request before any information is supplied.

11.4. A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

11.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

11.6. Where a request is manifestly unfounded, excessive or repetitive, the request may be refuse or a reasonable fee will be charged.

11.7. All fees will be based on the administrative cost of providing the information.

11.8. All requests will be responded to without delay and at the latest, within one month of receipt.

11.9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

11.10. Where a request is manifestly unfounded or excessive, the Trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

11.11. In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.

11.12. Any SAR received by a member of staff must be forwarded immediately to the Data Protection Officer in accordance with the Trust's Subject Access Request Procedure.

12. The right to rectification

12.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.

12.2. Where the personal data in question has been disclosed to third parties, the Trust will inform them of the rectification where possible.

12.3. Where appropriate, the Trust will inform the individual about the third parties that the data has been disclosed to.

12.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

12.5. Where no action is being taken in response to a request for rectification, the Trust will explain the reason for this to the individual, and will inform them of their right to complain to the ICO and to a judicial remedy.

12.6. Any request received by a member to exercise a data protection right must be forwarded immediately to the Data Protection Officer.

13. The right to erasure

13.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

13.2. Individuals have the right to erasure in the following circumstances:

· Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed

· When the individual withdraws their consent

· When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing

· The personal data was unlawfully processed

· The personal data is required to be erased in order to comply with a legal obligation

· The personal data is processed in relation to the offer of information society services to a child.

13.3. The Trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

· To exercise the right of freedom of expression and information

· To comply with a legal obligation for the performance of a public interest task or exercise of official authority

· For public health purposes in the public interest

- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

13.4. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

13.5. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

13.6. Where personal data has been made public within an online environment, the Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

13.7. Any request received by a member to exercise a data protection right must be forwarded immediately to the Data Protection Officer.

14. The right to restrict processing

14.1. Individuals have the right to block or suppress the Trust's processing of personal data.

14.2. In the event that processing is restricted, the Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

14.3. The Trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Trust has verified the accuracy of the data
- Where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the Trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

14.4. If the personal data in question has been disclosed to third parties, the Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

14.5. The Trust will inform individuals when a restriction on processing has been lifted.

14.6. Any request received by a member to exercise a data protection right must be forwarded immediately to the Data Protection Officer.

15. The right to data portability

15.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

15.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

15.3. The right to data portability only applies in the following cases:

. To personal data that an individual has provided to a controller

. Where the processing is based on the individual's consent or for the performance of a contract

. When processing is carried out by automated means

15.4. Personal data will be provided in a structured, commonly used and machine-readable form.

15.5. The Trust will provide the information free of charge.

15.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

15.7. The Sea View Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

15.8. In the event that the personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual.

15.9. The Trust will respond to any requests for portability within one month.

15.10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

15.11. Where no action is being taken in response to a request, the Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the ICO and to a judicial remedy.

15.12. Any request received by a member to exercise a data protection right must be forwarded immediately to the Data Protection Officer.

16. The right to object

16.1. The Trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

16.2. Individuals have the right to object to the following:

· Processing based on legitimate interests or the performance of a task in the public interest

· Direct marketing

· Processing for purposes of scientific or historical research and statistics.

16.3. Where personal data is processed for the performance of a legal task or legitimate interests:

· An individual's grounds for objecting must relate to his or her particular situation.

· The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

16.4. Where personal data is processed for direct marketing purposes:

· The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.

· The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

16.5. Where personal data is processed for research purposes:

· The individual must have grounds relating to their particular situation in order to exercise their right to object.

· Where the processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.

16.6. Where the processing activity is outlined above, but is carried out online, the Trust will offer a method for individuals to object online.

16.7. Any request received by a member to exercise a data protection right must be forwarded immediately to the Data Protection Officer.

17. Privacy by design and privacy impact assessments

17.1. The Trust will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

17.2. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

17.3. DPIAs will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to The Sea View Trust's reputation which might otherwise occur.

17.4. A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

17.5. A DPIA will be used for more than one project, where necessary. High risk processing includes, but is not limited to, the following:

· Systematic and extensive processing activities, such as profiling

· Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

17.6. The Trust will ensure that all DPIAs include the following information:

· A description of the processing operations and the purposes

· An assessment of the necessity and proportionality of the processing in relation to the purpose

· An outline of the risks to individuals

· The measures implemented in order to address risk

17.7. Where a DPIA indicates high risk data processing, the Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

18. Data breaches

18.1. The term **'personal data breach'** refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

18.2. The Executive Leader will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

18.3 All staff must report any actual or suspected personal data breach to the DPO immediately in accordance with the Data Breach Policy.

18.4. Where a breach is likely to result in a risk to the rights and freedoms of individuals, Information Commissioner's Office (ICO) will be informed.

18.5. All notifiable breaches will be reported to the ICO within 72 hours of the Trust becoming aware of it.

18.6. The risk of the breach having a detrimental effect on the individual, and the need to notify the ICO, will be assessed on a case-by-case basis.

18.7. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust will notify those concerned directly.

18.8. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the ICO.

18.9. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

18.10. Effective and robust breach detection, investigation and internal reporting procedures are in place at the Trust, which facilitate decision-making in relation to whether the ICO or the public need to be notified.

18.11. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

18.12. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

19. Data security

19.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

19.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

19.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

19.4. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

19.5. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

19.6. All electronic devices are password-protected to protect the information on the device in case of theft.

19.7. Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.

19.8. Staff and governors will not use their personal laptops or computers for Trust purposes.

19.9. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

19.10. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

19.11. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

19.12. When sending confidential information by fax or email staff will always check that the recipient is correct before sending.

19.13. When screening sharing on electronic devices, staff will always check that confidential or personal information cannot be viewed by others viewing the screen.

19.14. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Trust premises accepts full responsibility for the security of the data.

19.15. Before sharing data, all staff members will ensure:

· They are allowed to share it.

· That adequate security is in place to protect it.

· Who will receive the data has been outlined in a privacy notice.

19.16. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Trust containing sensitive information are supervised at all times.

19.17. The physical security of the Trust's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

19.18. The Sea View Trust takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

19.19. The Data Protection Officer is responsible for continuity and recovery measures are in place to ensure the security of protected data.

20. Publication of information

20.1. The Sea View Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

· Policies and procedures

· Annual reports

· Financial information

20.2. Classes of information specified in the publication scheme are made available quickly and easily on request.

20.3. The Sea View Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.

20.4. When uploading information to the Trust website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

21. CCTV and photography

21.1. The Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

21.2. The Trust notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

21.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

21.4. All CCTV footage will be kept in line with the Trust's Surveillance and CCTV policy for security purposes for (up to a maximum of 60 days); the Data Protection Officer is responsible for ensuring the records are secure.

21.5. The Trust will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

21.6. If the Trust wishes to use images/video footage of pupils in a publication, such as the Trust website, prospectus, or recordings of Trust plays, written permission will be sought for the particular usage from the parent of the pupil.

21.7. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.

22. Data retention

22.1. Data will not be kept for longer than is necessary in line with the Trust's Record Management Policy.

22.2. Unrequired data will be deleted as soon as practicable.

22.3. Some educational records relating to former pupils or employees of the Trust may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

22.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

23. DBS data

23.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

23.2. Data provided by the DBS will never be duplicated.

23.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

24. Training

24.1. We are required to ensure all staff have undergone adequate training to enable them to comply with data protection law. We must also regularly test our systems and processes to assess our compliance.

24.2. You must undergo all mandatory data protected related training in accordance with the Trust's training requirements.

25. Policy review

25.1. This policy is reviewed every two years by the Data Protection Officer and the Executive Leader.

25.2 The next scheduled review date for this policy is September 2025.

ANNEX ONE

Specia Category Data Policy

Introduction

1.1 This policy is intended to clearly set out the requirements of the UK General Data Protection Regulation (the **UK GDPR**) and the Data Protection Act 2018 (**DPA 2018**) which are relevant to Sea View Trust's (**the Trust**) use of sensitive personal data, known as "**special category data**".

1.2 It applies to all special category data which is processed on behalf of the Trust as part of your employment and also the special category data of pupils and parents which is also processed on behalf of the Trust.

1.3 This policy has been formulated to meet the requirement of the Data Protection Act 2018 (DPA 2018) that an appropriate policy document be in place where processing special category data and criminal convictions data in certain circumstances.

Definitions and Scope

2.1 For the purposes of this policy:

. **Personal data** means any information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

. **Processing** means any operation performed upon personal information. This includes collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available or destruction. This definition incorporates all automated data, manual data (held on personnel file) or other recorded data e.g., photographic film, video or tape recordings.

. **Employee** means an individual who is subject to personal data in the employment relationship. It applies to any current, past or prospective individual who has entered into, or intends to enter into a contract of employment. It also includes contractors operating on Trust premises, agency staff and students undergoing work placements.

. **Special category data** means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

. **Criminal convictions data** means personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

Employee Special Category Data

3.1 The UK GDPR and the DPA 2018 sets out strict rules about the way in which special category and criminal convictions data are collected, accessed, used and disclosed. Some of the Schedule 1 conditions in the Data Protection Act 2018 for processing special category data require us to have an appropriate policy document in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 of the UK GDPR and policies regarding the retention and erasure of special category data. This policy explains our processing and satisfies the requirements of Schedule 1, Part 4 of the Data Protection Act 2018.

3.2 We process the special category data and criminal convictions data of employees under the UK GDPR on the following bases:

. Article 9(2)(a) – explicit consent.

. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Trust or an individual in connection with employment, social security or social protection.

. Article 9(2)(c) – where processing is necessary to protect the vital interests of an individual.

. Article 9(2)(g) – for reasons of substantial public interest.

. Article 9(2)(f) – for the establishment, exercise or defence of legal claims.

3.3 We process the special category and criminal conviction data of employees for the following purposes:

. assessing an individuals' fitness to work

. assessing an individual's suitability to work within an education setting

. complying with health and safety obligations

. complying with our legal obligations to safeguard children and young people in accordance with Keeping Children Safe in Education statutory guidance

. complying with the Equality Act 2010

. checking applicants' and employees' right to work in the UK

. verifying that candidates are suitable for employment or continued employment.

Pupil and Parent Special Category Data

4.1 We process the special category data and criminal convictions data of pupils and parents under the UK GDPR on the following bases:

. Article 9(2)(a) – explicit consent.

. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Trust or an individual in connection with employment, social security or social protection.

. Article 9(2)(c) – where processing is necessary to protect the vital interests of an individual.

. Article 9(2)(g) – for reasons of substantial public interest.

. Article 9(2)(f) – for the establishment, exercise or defence of legal claims.

Compliance with the Data Protection Principles

5.1 The UK GDPR requires personal data to be processed in accordance with the six principles set out in Article 5(1) UK GDPR. Article 5(2) UK GDPR requires organisations to be able to demonstrate compliance with Article 5(1) UK GDPR.

5.2 We comply with the principles relating to processing of special category and criminal convictions data set out in the UK GDPR which require personal data to be:

Lawful, Fair and Transparent

5.3 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the individual.

5.4 We will only process personal data fairly and lawfully and for specified purposes. We will only process special category data if we have a legal ground for processing as set out in the UK GDPR and one of the specific processing conditions relating to special category data in the Data Protection Act 2018 applies.

5.5 When collecting special category and criminal convictions data, we will provide individuals with a privacy notice setting out all the information required by the UK GDPR in a privacy notice which is concise, transparent, intelligible, easily accessible and in clear plain language which can be easily understood.

5.6 We have identified and documented the legal grounds and specific processing condition for processing special category data as follows:

Employees

Special Category Data	**Lawful Basis for Processing Special Category Data**	**Processing Condition for Special Category Data**
Health Information	Compliance with a legal obligation (*Article 6 (1)(c)*) or necessary for the performance of a contract with the individual (*Article 6(1)(b)*).	Necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or

		the individual in connection with employment, social security or social protection. (*Paragraph 1(1)(a), Schedule 1, DPA 2018*.)
Racial or ethnic origin, religious and sexuality data	Compliance with a legal obligation (*Article 6(1)(c)*).	Necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or an individual in connection with employment, social security or social protection. (*Paragraph 1(1)(a), Schedule 1, DPA 2018*.)
Equal opportunities data	Compliance with a legal obligation (*Article 6(1)(c)*).	Necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or an individual in connection with employment, social security or social protection. (*Paragraph 1(1)(a), Schedule 1, DPA 2018*.) Necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained. (*Paragraph 8(1)(b), Schedule 1, DPA 2018*.)
Criminal Offences Data	Compliance with a legal obligation (*Article 6(1)(c)*).	Necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or an individual in connection with employment, social security or social protection.

		(*Paragraph 1(1)(a), Schedule 1, DPA 2018*.) Meets one of the substantial public interest conditions set out in Part 2 of Schedule 1 to the DPA 2018 (such as preventing or detecting unlawful acts). (*Paragraph 10(1), Schedule 1, DPA 2018*.)

Pupils and Parents

Special Category Data	**Lawful Basis for Processing Special Category Data**	**Processing Condition for Special Category Data**
Health Information	Compliance with a legal obligation (*Article 6 (1)(c)*) or necessary for the performance of a contract with the individual (*Article 6(1)(b)*).	Meets one of the substantial public interest conditions set out in Part 2 of Schedule 1 to the DPA 2018 (such as preventing or detecting unlawful acts, safeguarding children or vulnerable adults). (*Paragraph 10(1), Schedule 1, DPA 2018*.)
Racial or ethnic origin, religious and sexuality data	Compliance with a legal obligation (*Article 6(1)(c)*).	Necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or an individual in connection with employment, social security or social protection. (*Paragraph 1(1)(a), Schedule 1, DPA 2018*.)
Equal opportunities data	Compliance with a legal obligation (*Article 6(1)(c)*).	Necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to

		enabling such equality to be promoted or maintained. (*Paragraph 8(1)(b), Schedule 1, DPA 2018*.)
Criminal Offences Data	Compliance with a legal obligation (*Article 6(1)(c)*).	Meets one of the substantial public interest conditions set out in Part 2 of Schedule 1 to the DPA 2018 (such as preventing or detecting unlawful acts). (*Paragraph 10(1), Schedule 1, DPA 2018*.) Meets one of the substantial public interest conditions set out in Part 2 of Schedule 1 to the DPA 2018 (such as preventing or detecting unlawful acts, safeguarding children or vulnerable adults). (*Paragraph 10(1), Schedule 1, DPA 2018*.)

Purpose Limitation

5.7 All personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

5.8 We will only collect personal data for specified purposes and will inform individuals what those purposes are in a published privacy notice.

Data Minimisation

5.9 Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

5.10 We will only collect or disclose the minimum personal data required for the purpose for which the data is collected or disclosed. We will ensure that we do not collect excessive data and that the personal data collected is adequate and relevant for the intended purposes.

Accuracy

5.11 Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

5.12 We will ensure that the personal data we hold and use is accurate, complete, kept up to date and relevant to the purpose for which it is collected by us. We check the accuracy of any

personal data at the point of collection and at regular intervals afterwards. We take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

Storage Limitation

5.13 We only keep personal data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where we have a legal obligation to do so. Once we no longer need personal data it shall be deleted or rendered permanently anonymous.

5.14 We maintain a Records Management Policy to ensure personal data is deleted after a reasonable time has elapsed for the purposes for which it was being held, unless we are legally required to retain that data for longer.

5.15 We will ensure individuals are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

Security, Integrity and Accountability

5.16 Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.17 We will implement and maintain reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of or damage to personal data.

Accountability

5.18 We are responsible for, and able to demonstrate compliance with these principles. In particular, we shall:

. Ensure that records are kept of all personal data processing activities, and that these are provided to the Information Commissioner on request;

. Carry out a data protection impact assessment for any high-risk personal data processing to understand how processing may affect individuals and consult the Information Commissioner if appropriate;

. Ensure that a Data Protection Officer is appointed to provide independent advice and monitoring of personal data handling, and that the Data Protection Officer has access to report to the highest management level;

. Have internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with the UK GDPR and the Data Protection Act 2018.

Policies on Retention and Deletion

6.1 We take the security of special category data very seriously. We have administrative, physical and technical safeguards in place to protect personal data against unlawful or unauthorised processing, or accidental loss or damage. We will ensure, where special category data is processed that:

. The processing is recorded, and the record sets out, where possible, a suitable time period for the safe and permanent erasure of the different categories of data in accordance with our Records Management Policy.

. Where we no longer require special category data for the purpose for which it was collected, we will delete it or render it permanently anonymous as soon as possible.

. Where records are destroyed we will ensure that they are safely and permanently disposed of in accordance with our Records Management Policy.

. Individuals receive a privacy notice setting out how their personal data will be handled when we first obtain their personal data, and this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. Our pupil and parents privacy notice is also available on our website and on our intranet for employees.

Review

7.1 This policy is reviewed every two years by the Data Protection Officer and the Executive Leader.

7.2 The next scheduled review date for this policy is September 2025.