INDEPENDENT SCHOOLS INSPECTORATE

DATA PROTECTION POLICY

LAST REVIEW:	**October 2024**
POLICY OWNER:	**Chief Operating Officer**
APPROVED BY:	**Finance and Infrastructure Committee**
NEXT REVIEW:	**October 2026**

Contents

Policy statement

1. Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities, we will collect, store and process personal data and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

2. This policy applies to all employees, volunteers, workers, contractors, inspectors and all other third parties working at, with, or for ISI ("Data users").

3. Data users are obliged to comply with this policy when processing personal data on our behalf and need to implement appropriate practices, processes, controls and training to ensure compliance. Any breach of this policy may result in disciplinary action for employees, or the immediate termination of a contractor agreement, or no further deployment of an inspector.

Safeguarding

3. Whilst organisations and individuals have a duty to process personal data fairly and lawfully, data protection is not a barrier to sharing information where the failure to do so would result in a child being placed at risk of harm.

4. Where safeguarding or child protection concerns arise, we will act in the interests of the child. In such circumstances, ensuring the well-being of the child may involve sharing confidential information with relevant child protection bodies. For further guidance, please see the government's non-statutory advice: Information sharing advice for safeguarding practitioners If in doubt, please consult the Senior Director (Safeguarding, Legal and Complaints), or in their absence, the Chief Executive Officer-Chief Inspector. Please also see Annex B below in relation to ISI's approach to handling special category data arising from safeguarding concerns.

About this policy

4. The types of personal data that ISI or those acting on our behalf ("We", "Us", "Our") may be required to handle include information about current, past and prospective employees, directors, inspectors or other contractors, suppliers, parents, pupils/students and staff from schools and further education institutions, public bodies and other third parties with which we communicate. Personal data, which may be held on paper, or on a computer or other media, is subject to legal safeguards specified in the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("DPA 2018") and other regulations.

5. This policy and any other relevant documents referred to in this policy set out the basis on which we will process personal data and the rules that must be followed when we collect or otherwise obtain, handle, process (including sharing), transfer, store and delete personal data.

Responsibility

6. The Chief Operating Officer is accountable for data protection.

7. The Head of Information Technology is responsible for ensuring compliance with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Head of Information Technology at dp@isi.net

Definition of data protection terms

8. **Criminal offence data** is personal data relating to criminal convictions and offences.

9. **Data** is information which is stored electronically, in hard copy or in another medium such as video or audio file, including certain paper-based filing systems

10. **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the UK GDPR and the DPA 2018. ISI is the data controller of all personal data used in our business for our own inspection and commercial purposes. In relation to any personal data processed for the purpose of school inspections, both ISI and the relevant reporting inspector are data controllers.

11. **Data privacy impact assessments** (DPIA)s are risk assessments carried out to identify and minimise the data protection risks of a project. The UK GDPR requires DPIAs to be carried out in certain circumstances which are described below.

12. **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition, but it would include team inspectors, directors and/or suppliers who handle personal data on ISI's behalf.

13. **Data users** are those of our employees and contractors whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times**.**

14. **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

15. **Personal data** means data relating to a living individual who can be directly or indirectly identified from that data (or from that data and other available information). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour. Personal data also includes online identifiers and location data. Personal data that has been pseudonymised may be personal data if it can be attributed to a particular individual.

16. **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

17. **Processing** is any activity that involves use of the personal data. It includes obtaining, recording or holding the personal data, or carrying out any operation or set of operations on the personal data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

18. **Special category personal data** is sensitive data, which includes personal data concerning a natural person's health, sex life or sexual orientation or personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships, and genetic or biometric data.

19. **Third country** means a country outside the UK.

Principles relating to processing of personal data

20. Anyone processing personal data must comply with the six enforceable principles set out in the UK GDPR. These provide that personal data must be:

    i. Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).

    ii. Collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).

    iii. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization).

    iv. Accurate and, where necessary, kept up to date (accuracy).

    v. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (storage limitation).

    vi. Secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (security, integrity and confidentiality).

21. Everyone is required to ensure (and must be able to demonstrate) that the above principles are followed (accountability).

Lawful, fair and transparent processing

22. The UK GDPR and the DPA 2018 are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in Article 6 UK GDPR. When special category and/or criminal offence data personal data is being processed, additional conditions must be considered. Please refer to Annex B for information.

23. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met. ISI relies on different legal grounds depending on the category of personal data being processed. Each new category of data is reviewed on a case-by-case basis. Please see Annex B for details.

    i. For ISI to rely on consent, it must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as a written statement or an oral statement. When the processing has multiple purposes, consent should be given for each of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use for which it is provided. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. A Data Subject must be easily able to withdraw consent at

any time and withdrawal must be promptly honoured. Consent will need to be refreshed if you intend to process personal data for a purpose which was not disclosed when the Data Subject first consented.

ii. For ISI to rely on the legitimate interests ground, ISI must balance these against the interests or fundamental rights and freedoms of the data subject, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.

24. Any information and communications addressed to a child should be in such a clear and plain language that the child can easily understand and be age appropriate.

Processing for specified, explicit and legitimate purposes

25. In the course of our business, we may collect and process a range of personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, public bodies, schools, associations, parents, pupils, inspectors, sub-contractors, payment and delivery services, credit reference agencies and others).

26. We will only process personal data for the specific purposes set out in Annex A or for any other purposes specifically permitted by the UK GDPR and the DPA 2018.

Adequate, relevant and limited to what is necessary

27. We will only collect personal data to the extent that it is required for the specific purposes set out in Annex A or another specific purpose notified to the data subject. The processing of personal data for purposes other than those for which the personal data were initially collected will be allowed only where the processing is compatible with the purposes for which the personal data were initially collected.

Accurate data

28. We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date data.

Timely processing and record keeping

29. We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, anonymise, aggregate or erase from our systems, all data which is no longer required in line with the retention schedule at Annex A.

30. ISI maintains a record of processing activities under its responsibility. This record includes: the purposes of the processing; a description of the categories of data subjects and of the categories of personal data; the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in certain circumstances, the documentation of suitable safeguards; where possible, the envisaged time limits for erasure of the different categories of data; and, where possible, a general description of the technical and organisation security measures.

Personal data security

31. We will take appropriate security measures against unlawful access to, unauthorised processing of personal data, and against the accidental loss of, or damage to or destruction of, personal data.

32. We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if it agrees to comply with those procedures and policies, or if it puts in place alternative adequate measures giving rise to the same level of protection.

33. We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

    i. **Confidentiality** means that only people who are authorised to use the data can access it, but see also clause 2 above.

    ii. **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

    iii. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on ISI's central cloud based computer system, on premises file stores or in office filing cabinets instead of individual PCs or home offices.

34. Security procedures include

    i. **Entry controls.** Entrance to ISI is by entrance phone, security fob and security-pad. Any stranger seen in entry-controlled areas should be reported to Business Support

    ii. **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal data is always considered confidential.)

    iii. **Methods of disposal.** Paper documents containing confidential information, such as personal data, should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

    iv. **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock their PC when it is left unattended.

    v. **Network security.** Passwords for access to the company network and the ISI online portals are confidential and must not be revealed to anyone else, including the Information Services team. The Information Services team must be informed of any concerns that a password has been compromised. A password reset will be arranged. Multi factor authentication (MFA) is in place for the majority of applications holding sensitive data.

    All software installations, downloads, CDs or USB sticks must be authorised by the Information Services team before they are used on any network PC or laptop.

    The antivirus software on company PCs updates automatically.

ISI reserves the right to regularly audit company PCs and servers to monitor content stored on them and to monitor the performance of the network.

All actual or suspected breaches of data, or any system, are to be immediately reported to the Information Services team.

vi. **Deletion of unnecessary or irrelevant data.** Please see Annex A.

vii. **Additional security measures in relation to special category data and criminal offence data.** Please see Annex B.

Personal data breach response

35. ISI will deal with personal data breaches in accordance with our Personal Data Breach Policy.

Data protection impact assessments

36. The GDPR requires data protection impact assessments (DPIAs) to be carried out for processing operations that present a high risk to individuals due to the nature or scope of the processing operation. Please contact the Head of Information Technology if you have queries about whether a DPIA is required in respect of any existing or new operations.

37. Examples of processing operations which are likely to require a DPIA are:
    i. Use of new technologies or changing technologies
    ii. Automated processing including profiling and automated decision making
    iii. Large scale processing of special category personal data

38. A DPIA must include:
    i. A description of the processing and its purposes
    ii. And assessment of the necessity and proportionality of the processing relating to its purpose
    iii. An assessment to the risks to individuals
    iv. The risk mitigation measures in place

Processing and notifying in line with data subjects' rights

39. If we collect personal data directly from data subjects, it shall be transparent to data subjects that personal data concerning them is collected, used, consulted or otherwise processed and the extent to which the personal data is or will be processed.

40. Any information and communication relating to the processing of personal data shall be easily accessible and easy for data subjects to understand, and clear, concise and plain language will be used.

41. If we collect personal data directly from data subjects, we will inform them about:

    i. Our identity and contact details.

    ii. The purpose or purposes for which we intend to process their personal data and the legal basis for the processing. This will include, where relevant, details of the legitimate interests we are pursuing.

iii. The types of third parties, if any, with which we will share or to which we will disclose that personal data.

iv. Where applicable, the fact that we intend to transfer personal data to a third country or international organisation.

v. The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

vi. The existence of the right to request from ISI access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability.

vii. The right to withdraw consent, if consent is the lawful ground being relied upon for processing. To withdraw consent, data subjects can contact ISI via email: dp@isi.net ; by phoning: 020 7600 0100; or by writing to: Head of Information Technology, ISI, CAP House, 9-12 Long Lane, London EC1A 9HA.

viii. The right to lodge a complaint with a supervisory authority.

ix. Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

x. The right to request information as to the source of the personal data where it has not been collected from the data subject.

42. If we receive personal data about a data subject from other sources, such as in the course of inspection activity, it will be retained for no longer than necessary, in accordance with Annex A. Thereafter it will be deleted or destroyed confidentially.

43. Except where personal data is processed in the course of inspection activity, we will also inform data subjects whose personal data we process that we are the data controller with regard to that data, and who the Data Protection Compliance Manager is.

Dealing with subject access requests and requests for rectification and erasure

44. ISI will deal with requests for rectification and erasure in accordance with its policy on Rectification and Erasure requests.

Transferring personal data to a country outside the EEA

46. We may transfer any personal data we hold to a country outside the UK.

47. Personal data is transferred when it is sent, transmitted, viewed or accessed in or to a different country.

48. We will only transfer personal data outside of the UK provided that one of the following conditions applies:

i. The country to which the personal data is transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

ii. Appropriate safeguards are in place such as standard contractual clauses approved for use in the UK;

iii. The data subject has given explicit consent to the proposed transfer after being made aware of any potential risk;

iv. The transfer is necessary for one of the reasons set out in the UK GDPR and the DPA 2018, including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims, or to protect the vital interests of the data subject;

v. The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

49. Subject to the requirements in clause 48 above, personal data we hold may also be processed by staff, inspectors, suppliers, contractors, schools operating outside the UK, or those providing support services to them.

Disclosure and sharing of personal data

50. We may share personal data we hold with any member of our group, which includes any subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

51. We will only share personal data with third parties where certain safeguards and contractual arrangements have been put in place to ensure an adequate level of protection, namely:

i. they have a need to know the information for the purposes of providing the contracted services;
ii. sharing the personal data complies with the Privacy Notice provided to the data subject and, if required, their consent has been obtained;
iii. the third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place;
iv. the transfer complies with any applicable cross-border transfer restrictions; and
v. a fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.

52. We may also disclose personal data we hold to third parties:

i. in the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.
ii. if we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.
iii. if we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or the safety of children at the schools we inspect, our employees, contractors, inspectors, or others. This includes exchanging information with other companies, organisations and public

bodies for the purposes of child protection, prevention or detection of crime, fraud protection and credit risk reduction.

Changes to this policy

53. We reserve the right to change this policy at any time. When we make significant changes, we will notify our staff and data users via email unless specifically agreed otherwise.

Table of key changes

Date of review	Paragraph number	Amendments
October 2024	4	Updated link to *Information Sharing* website
	6-7	Updated titles relating to responsibilities
	21	Clarity that everyone is required to ensure that data protection principles are followed
	31	Including 'access to'
	33 iii	Include reference to cloud based storage
	34 iv	Amend reference to locking laptops rather than logging off
	34 v	New reference to multi factor authentication and reference to reporting of breaches to include potential breaches of data
	36	Update data compliance manager to Head of Information Technology
	41 vii	Updated contact details
	Appendix A	All lines in retention schedule reviewed and updated in accordance with changes to the ISI portal

Annex A – Legal Basis and Retention Schedule

	Category	Legal basis	Type of document / information	Retention instructions for employees	Retention instructions for inspectors
1.	**All concerns**	Substantial public interest. **NB this may include special category data (see Annex B below)**	**Portal record: Notes, emails, attachments, saved documents (including any videos or audio files) relating to concerns, including referrals to and correspondence with the DfE, local authorities, police and other agencies.**	• Annually delete concerns records in the ISI portal relating to schools that have undergone a routine inspection in the prior year, retaining the number and type of concerns only.	No information to be held by inspectors
2.	**All concerns**	Substantial public interest. **NB this may include special category data (see Annex B below)**	**Safeguarding team record: school safeguarding summaries (SSS) and sensitive information that is not uploaded to the portal due to sensitivity of personal data**	• Annually delete School safeguarding summaries (SSS) held on the safeguarding drive/SharePoint site relating to schools that have undergone a routine inspection in the prior year retaining the number and type of concerns only.	n/a
3.	**Inspection evidence**	Public interest Legal obligation	**All evidence bases including records of evidence and inspection activity forms, documents, drafts, emails, paperwork, forms, notes, questionnaire responses, records of evidence and any other records including pre-inspection information and papers**	• Evidence bases on the portal will be retained from the **start** of the previous framework. (ie deleting all evidence from any frameworks prior to 1st April 2016).	Anything saved locally must be deleted immediately following completion of the onsite inspection and once saved to an Inspection Activity Form.
4.	**Inspection evidence**	Public interest Legal obligation	**Teamroom data**	• Teamroom data will be deleted once an inspection report is published	n/a
5.	**Inspection reports**	Public interest Legal obligation	**Published inspection reports.**	• Reports published from September 2017 will remain publicly available on the ISI website **indefinitely**. One electronic copy of all historic reports should be archived and kept for reference purposes **indefinitely**.	n/a

	Category	Legal basis	Type of document / information	Retention instructions for employees	Retention instructions for inspectors
6.	**Inspector details**	Contract	**Inspector contact details, DOB, CVs / career history, photographs, application, vetting checks (other than DBS checks), copies or details of ID, contracts, performance notes, medical fitness declaration or other personal data relevant to inspections.**	• **Retain** whilst inspector is active. • On being made inactive, ISI **system auto-creates 'skeleton file'** which contains 1 inspector name, 2. inspector recruitment checks record, 3. links to all inspections the inspector has undertaken • All other data, including documents related to their profile, will be deleted with their portal user accounts. • *Note: for any inspector who has been made inactive and has never been on inspection, all information will be deleted ie a skeleton record will* ***not*** *be created.*	n/a
7.	**Inspector details**	Legitimate interest	**Name and dates of inspections**	• On being made inactive, auto-create 'skeleton file' which contains 1. inspector name 2. inspector recruitment checks record 3. links to all inspections the inspector has undertaken • All other data, including documents related to their profile, will be deleted with their portal user accounts.	n/a
8.	**Inspector details 'skeleton' file**	Legitimate interest	**Name, links to inspections, record of recruitment checks carried out**	• Retain for 20 years from the date of their last inspection.	
9.	**Inspector details**	Contract	**Evaluation/feedback forms completed post inspection by schools, inspection team and RI.**	• Retain CIEFs relating to individual inspectors while inspecting. On ceasing inspection, delete CIEFs about (but not completed by) the individual inspector.	n/a

	Category	Legal basis	Type of document / information	Retention instructions for employees	Retention instructions for inspectors
10.	**Inspector details**	Contract	**Bank details, invoicing, payment, expenses claims and related paperwork.**	• Retain bank details on accounting software (Xero) while active. Once made inactive, retain until completion of next audit cycle then permanently delete/shred.	n/a
11.	**Inspector details**	Legal obligation	**DBS check details**	• Only retain certificate reference number and date of issue in the skeleton record. - i.e. retain data held in the 'Inspector Checks' record, but no related DBS documentation will be retained. • Where an individual does not have a clear DBS record but is still deployed, a risk assessment will be held securely by the Safeguarding team. Any such risk assessment will be retained for the inspector's period inspecting for ISI and delete when made inactive.	n/a
12.	**Inspector details**	Contract	**Training records on the portal and LMS**	• Training records on the LMS and the ISI portal will be deleted when an inspector is made inactive.	
13.	**Inspector recruitment**	Consent	**Unsuccessful applications and related paperwork**	• Retain securely for **up to 12 months** following date of rejection and then delete all personal data.	n/a
14.	**School portal users**	Consent	**Name, display name, user name, email address, telephone number of the school**	• Retain while user account active. Delete the account after two years' inactivity, or sooner if user informs ISI they no longer require access.	n/a
15.	**ISI personnel information**	Contract	**Staff contact details, date of birth, next of kin, CVs / career history, declaration of interest form, contracts, appraisal / performance review**	• Retain securely whilst the individual is an employee. Following the end of employment retain for **six years** and then permanently delete/shred.	n/a
16.	**ISI personnel information**	Legal obligation	**DBS checks, right to work checks**	• Only retain certificate reference number and date of issue (certificates are seen but no copies are taken).	n/a

	Category	Legal basis	Type of document / information	Retention instructions for employees	Retention instructions for inspectors
				• Where an individual does not have a clear record details will be held securely by the HR Team and known by the Chief Executive Officer-Chief Inspector. • Delete details **six years** after staff member stops working for ISI. A record of the check is held by the DBS outsourced checker for seven years for audit and archive purposes.	
17.	**ISI personnel information**	Contract	**Training records on the LMS**	• Retain securely for six years after date of leaving.	
18.	**ISI personnel information**	Contract	**Holiday and sickness records, working from home record, appraisals as held on PeopleHR and/or on ISI systems including paper copies, photos.**	• Retain securely for up to **six years** and then permanently delete/shred.	n/a
19.	**ISI personnel information**	Contract	**Salary details, PAYE information, national insurance number & pension information.**	• Retain securely whilst the individual is an employee. Following the end of employment retain for **six years** and then permanently delete/shred.	n/a
20.	**ISI recruitment**	Consent	**Unsuccessful applications and related paperwork.**	• Delete within **six months** after the closing date unless otherwise agreed.	n/a
21.	**Schools**	Public interest	**School ISI portal record (contains contact details for head + bursar).**	• Keep up to date details as long as school is inspected by ISI. • Where a school is no longer to be inspected by ISI IT team to remove any information relating to specific individuals within **six months.** • Where a school is merged, the unique record of the original schools are, as appropriate, retained as historic, and linked to the new school record.	n/a
22.	**Complaints**	Legitimate interest	**Any documents, emails, notes, correspondence etc. relating to a complaint about ISI / an inspection.**	• Retain for up to **six years** following date of closure of complaint and then permanently delete/shred.	Retain for a maximum of two months following date of closure of

	Category	Legal basis	Type of document / information	Retention instructions for employees	Retention instructions for inspectors
					complaint and then permanently delete.
23.	**General correspondence**	Legitimate interest	**Routine day-to-day correspondence - i.e. emails, letters, notes of meetings and phone calls.**	• Review and delete or file on an **annual** basis - only keep information that is still needed for ISI purposes - • i.e. ongoing communications, useful reference emails, records of decisions etc. All superfluous information should be deleted.	Review and delete or file on an **annual** basis. Only keep information that is still needed for ISI purposes - i.e. ongoing communications, useful reference emails, records of decisions etc. All superfluous information should be deleted.
24.	**School account information**	Legitimate interest	**Invoicing / payment details**	• Retain securely for **six years** and then permanently delete/ shred.	n/a
25.	**Board members' personal information**	Consent/ Legitimate interest	**Personal Information about board members (name, address, date of birth, record of DBS check)**	• Delete personal information within six months of leaving the Board. Names held on Companies House.	n/a
26.	**Board documentation**	Consent/ Legitimate interest	**Board meeting paperwork (minutes and records of resolutions passed otherwise than at general meetings)**	• Retain securely for **ten years** and then permanently delete/shred (as set out in Articles of Association)	n/a
27.	**ISI personnel information**	Contract	**ISI staff network logins and profiles (including record of use of internet and ISI systems).**	• Delete IT systems account six months after leaving.	n/a

	Category	Legal basis	Type of document / information	Retention instructions for employees	Retention instructions for inspectors
28.	**ISI personnel information**	Contract	**ISI phone call records (by phone number).**	• Retain securely for **six years** and then permanently delete.	n/a
29.	**Photos and videos**	Consent	**Stock images and videos used in ISI materials and training.**	• Ensure that relevant permissions / licences are sought for new images. Delete within two years of final use.	n/a

Annex B – Special category data and criminal offence data

(a) Special category data:

1. Safeguarding children is at the centre of ISI's role as a school inspectorate. A key part of this is the work of the Safeguarding Team. The Safeguarding Team is available as a point of contact for parents, teachers, pupils and other stakeholders to express any concerns in relation to schools. Such contact may be made via online form, or email. Concerns may include personal data including special category personal data (for example, information relating to protected characteristics, sensitive data such as family situation including social services or local authority involvement, safeguarding information, and information about special educational needs) and/or criminal offence data. Appropriate security measures are in place to ensure such information is only accessible by relevant individuals.

2. Substantial public interest

2.1 The collection of personal data relating to safeguarding concerns is considered by ISI to be in the substantial public interest.

2.2 ISI acknowledges that in some circumstances the information provided to ISI in relation to safeguarding concerns includes special category personal data about individuals who are not aware of ISI's processing. It is unlikely to be appropriate for ISI to inform such individuals as doing so could disrupt ISI's management of concerns for the purpose of inspection.

2.3 The DPA 2018 outlines that processing of personal information relating to individuals who are not aware of this processing can go ahead if the safeguarding derogation is met. ISI's processing meets with the DPA 2018's requirements as it is necessary to protect an individual under the age of 18 from neglect or physical, mental or emotional harm, or protecting the physical, mental or emotional well-being of an individual, and the processing is necessary for reasons of substantial public interest. The processing is carried out without the consent of the data subject because:

a. in the circumstances, consent to the processing cannot be given by the data subject;
b. in the circumstances, ISI cannot reasonably be expected to obtain the consent of the data subject to the processing; or
c. the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection of the individual raising the concern.

2.4 However, ISI operates a personal data minimisation approach. ISI requests that if personal data is provided to us in relation to individuals who are not aware of the processing, the information is kept to what is strictly necessary, and redacted where possible.

3. Security of special category data

3.1 **Portal – "Concerns" section:**

3.1.1 This area contains special category information about children, teachers, parents and other individuals.

3.1.2 Access will be limited to those who require access: the Safeguarding Team; the Quality Assurance Team; the Chief Executive Officer-Chief Inspector; the Senior Directors; the Head of Delivery; IT administrators (where necessary for example for the purposes of a subject access request) and the Reporting Inspector responsible for inspecting the relevant school.

3.1.3 There are three categories of concerns: open, closed and archived. The open concerns are ongoing and could be updated at any time, even after part or all of the concern has been considered on inspection. The closed concerns have been fully assessed and considered on inspection. The archived concerns have been fully assessed and the relevant school has been inspected, the retention period of six years has passed however, the decision has been made to keep the concern on file due to special circumstances.

3.2 **Safeguarding drive:** This mirrors the portal in terms of content and is accessible by the Safeguarding Team; the Chief Executive Officer-Chief Inspector; Senior Director (Safeguarding, Legal and Complaints).

3.3 **Safeguarding inbox:** This is accessible by the Safeguarding Team; IT administrators, Senior Director (Safeguarding, Legal and Complaints) and others on a short term basis as necessary (eg a Reporting Inspector). Emails are transferred to the ISI portal concerns section and deleted from the Safeguarding inbox by the Safeguarding Team within 30 calendar days following receipt.

3.4 **CJSM:** This is a very secure email system, usually used by the Safeguarding Team to transfer to or receive very sensitive information from local authorities.

(b) Criminal offence data

1. Inspection is defined as regulated activity in Schedule 4 of the Safeguarding Vulnerable Groups Act 2006 so far as the function gives the person the opportunity to have contact with children. It is a criminal offence for employers or voluntary organisations to knowingly employ a barred person in regulated activity. Therefore, ISI carries out enhanced Disclosure and Barring Service ("DBS") checks on all inspectors, members of staff and Board directors.

2. The legal basis for such processing is therefore that it is a legal obligation.

3. **Conditions for processing:** Processing of criminal offence data must meet a condition in Part 1, 2 or 3 of Schedule 1 of the DPA 2018. ISI's processing of criminal offence data meets this requirement because it (a) is necessary for the purposes of performing or exercising obligations imposed by law on the data controller in connection with employment and an appropriate policy documenting this is in place (a condition "relating to employment, health and research etc") and/or (b) is necessary for the safeguarding of children (a "substantial public interest" condition).

4. Additionally, consent of the data subject is always obtained before DBS checks are carried out.

5. **Appropriate policy document and additional safeguards:** This policy sets out ISI's data protection procedures and policy, including as regards the retention and erasure of personal data relating to criminal offences.