Independent Educational Services Ltd.

Data Protection Policy

Our Commitment:

Independent Educational Services is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA). https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

Changes to data protection legislation shall be monitored and implemented in order to remain compliant with all requirements.

The member(s) of staff responsible for data protection is: Shaun Major, Director

The school is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

General Statement
The school is committed to maintaining the above principles at all times.
Therefore the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so in an appropriate and secure manner
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

Notification:

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified immediately to the individual(s) concerned and the ICO.

Personal and Sensitive Data:

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

The principles of the Data Protection Act shall be applied to all data processed:

1. Processed fairly and lawfully

2. Obtained only for lawful purposes, and is not further used in any manner incompatible with those original purposes

3. Accurate and, where necessary, kept up to date,

4. Adequate, relevant and not excessive in relation to the purposes for which it is processed

5. Not kept for longer than is necessary for those purposes

6. Processed in accordance with the rights of data subjects under the DPA

7. Protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage

8. Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information

Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents/carers and pupils prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.
https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them.

Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:
https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacy-impact-assessments-code-published/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and these organisations shall provide evidence of the competence in the security of shared data.

Data Access Requests (Subject Access Requests):

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within 40 days and they should be made in writing to: Shaun Major

A charge may be applied to process the request.

https://ico.org.uk/media/for-organisations/documents/1586/personal_information_online_small_business_checklist.pdf
https://ico.org.uk/media/for-organisations/documents/1235/definition-document-schools-in-england.pdf

Photographs and Video:

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.

Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources without seeking prior permission.

It is the school's policy that external parties (including parents/carers) may not capture images of staff or pupils during such activities without prior consent.

Data Disposal:

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be deleted/destroyed in accordance with this policy.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance:
https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

Overview:

When a file is deleted, the operating system does not completely remove the file from the disk; rather, the file deletion removes only the reference to the file from the file system table. The file remains on the disk until a subsequent file is created over the original file. However, even after the file is overwritten, it is possible to recover data from the original file by studying the magnetic fields on the disk platter surface if the drive was manufactured before 2001. This is referred to as a "laboratory attack". Other drives may contain data that can be retrieved with specialized software. This is referred to as "deleted file retrieval". The only way to prevent these kinds of inadvertent file sharing or file access is to appropriately

clean (e.g., sanitize) the hard drive or other media by performing a data wipe or over-write, or to physically destroy the hard drive or other media before it reaches its next owner or destination. The required procedures for performing a data wipe or over-write, or for physically destroying the hard drive or other media, are set forth below.

Any official IES records must be appropriately retained/disposed of based on the IES's data protection policy prior to cleaning or destruction of the system, device, or media.

Overwriting Hard Drives or other Media:

The sanitization method for the media depends on the information stored on the media, the age of the media, and on its next destination. The following table should help decide how to handle a particular computer or device.

https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf, defines the terms and methods for sanitizing hard drives and other media.

Clearing: Overwriting the media

Purging: Magnetic erasure of the media

Destruction: Physical destruction of the media

Examples of Sensitive and Confidential Information include, but are not limited to, the following data types:

- National Insurance Numbers
- Student educational records
- Health care records
- Bank account and other financial information
- Research data
- Personnel data
- Other confidential or sensitive IES business information
- Proprietary software

If you need assistance removing data, or if you are not sure whether the data stored on a device is Sensitive or Confidential, please contact the IT Support Team for guidance.

New Location of Device	Data stored on Device	Recommendation
Same department	No Sensitive/Confidential data	Reformat or reimage
Another department or unit	No Sensitive/Confidential data	Reformat or reimage
Same department to staff with access to same information	Sensitive/Confidential data	Reformat or reimage
Same department to staff with lower access (or student worker)	Sensitive/Confidential data	Clear
Another department or unit	Sensitive/Confidential data	Clear
Recycling or disposal (including surplus)	All data	Clear
Drive manufacture date prior to 2001 or unknown	Sensitive/Confidential data	Purge
Non-functioning media	All data	Purge (magnetic); Destroy (solid state)

The most current research on data retrieval indicates a single pass of random data or zeros (Clearing) is all that is required to sanitize a functioning hard drive manufactured after 2001. Clearing the drive prevents deleted file retrieval. Laboratory attacks are not possible on modern hard drives.

Tools:

To properly clean your electronic media, please use the utility called "Darik's Boot and Nuke" (DBAN). This tool will create an easy-to-use cleaning floppy or CD that can be used in most computers. It will allow you to boot from the media and begin the cleaning process without needing to install any other software on the computer. DBAN allows you to choose a number of options.

Physical Destruction of Hard Drives or other Media:

If the computer system, electronic device, or electronic media will not be reused, physical destruction is an acceptable method of disposing of IES data. Individuals desiring to have a computer system, electronic device, or electronic media destroyed may contact the IT support team to arrange for drop-off or pick-up of their electronic waste.

Complaints:

Complaints about the above procedures should be made to the Directors who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.