For legitimate identification, safeguarding, education, support, management and other related purposes, Tute retains personal information about both staff and students. We acknowledge that data we retain is defined by the Data Protection Act 1998 as 'sensitive' in nature, it is therefore our policy to uphold high standards of privacy and protection.

**Our ICO Registration number is:** ZA097670
**Our nominated data protection officer is:** Philip Davies
**Our integrated data centres, provided through technology delivery partners, have ISO 27001/2 based policies, subject to annual review**

This policy and related practices exist to ensure we meet our legal obligations to students, staff and commissioning bodies. It provides protection from data security risks through unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

**Our personal data principles**

- We will be transparent about our collection of data and its intended purpose
- Only data that is relevant, adequate and not excessive to our purpose will be requested
- Data is requested for **our own purposes only**, will be securely stored and will be shared strictly in accordance with the Data Protection Act 1998
- Data will be regularly audited and maintained to ensure it is accurate and up to date
- Personal data shall be processed fairly and lawfully in accordance with schedules 2 and 3 of the Data Protection act 1998

**Schedule 2:** http://www.legislation.gov.uk/ukpga/1998/29/schedule/2
**Schedule 3:** http://www.legislation.gov.uk/ukpga/1998/29/schedule/3

- Personal data will be handled only in ways that the subject would reasonably expect and will be made available to them upon making a subject access request under the Data Protection Act 1998

**Staff guidelines**

- The only people with access to data will be those who need it for their work
- All staff must agree to our confidentiality policy and must not disclose information informally or to unauthorised people within the organisation or externally
- Staff will use strong passwords (8 characters in length and containing special symbols)
- Passwords must not be shared with colleagues
- Staff training is founded upon a best fit approach to the ICO checklist for small to medium sized businesses **(See Appendix 1)**
- Data protection training is included in our staff induction programme and is updated in accordance with relevant changes to legislation
- If they are unsure about any aspect of data protection, staff should seek the advice of our data protection officer
- If any member of staff is concerned that data security may have been breached they should inform the data protection officer immediately

**All staff are forbidden from holding personal data on their own devices**

**Security of electronic data**

- Computers used to store data are protected by strong user passwords
- Generic passwords are not used
- User privilege controls ensure access to data is appropriately restricted to those who need to know
- Firewalls, anti-virus software and anti-spyware are installed on all computers and are set to update automatically

- Information held on computer systems is subject to regular back-up stored separately from the computer
- All information is securely removed from the hard drive of old computers prior to disposal
- Personal information held electronically that would cause damage or distress if it were lost or stolen is encrypted or password protected
- All company laptops are securely stored when not in use and rooms equipped with computers are locked when not in use.

**Security of hard copy data**

- We aim to be as paper free as possible and minimise the amount of hard copy data retained
- Hard copies of personal and sensitive data are retained in lockable rooms within locked filing cabinets with restricted access by key members of staff
- Our clear desk policy ensures hard copy information is secured stored when not in use
- Our premises are alarmed and subject to regular checks.

**Secure transfer of data**

- Our platform offers a secure means of transferring information
- If sensitive information is shared by email, the content will be password protected or encrypted
- Staff are requested to consider privacy when sharing information by email **(see Appendix 2)**

**Security breaches**

- All breaches or suspected breaches of security or near misses are reported to the nominated data protection officer who will lead an investigation into the matter
- The ICO Personal data security breach log **(See Appendix 4)** is used to record all relevant information and remedial action taken
- The ICO will be informed within 24hours of detection of any security breach
- In the event of the loss of any unencrypted data, subscribers will be informed as follows:

    - Tute contact details
    - The estimated date of the breach
    - A summary of the incident
    - The nature and content of the personal data
    - Likely effect on the individual
    - Any measures you have taken to address the breach
    - How they can mitigate any possible adverse impact of the breach

- A full debrief will be carried out and preventative measures taken against repeated events
- Induction and training of staff will be reviewed as necessary

**Data Erasure and Retention**

- As an education provider we retain and dispose of data in accordance with the recommendations of the Records Management Service (RMS) Retention guidelines for schools **(See Appendix 3)**
- Data audit logs will be maintained on behalf of each commissioning body to document retention periods, access requests and deletion
- All confidential paper waste is disposed of by shredding
- Secure deletion methods are used; electronic memories are scrubbed clean or destroyed

**Data and Third Party Suppliers**

- Data will only be shared with Tute's partners for the purposes of technical troubleshooting on a needs-must basis i.e. 2nd line support or whereby Tute use a third party service to host electronic data
- All third-parties are subject to rigorous diligence and accreditation checks to ensure compliance with the treatment of all client data and as such, will be bound to the same levels of confidentiality as the customer may expect from Tute
- Clients are informed of Tute's technology partners and their role in the business operation during the on-boarding process

**This policy is further reinforced by additional Tute policies as follows:**

| | |
|---|---|
| **Confidentiality Policy:** | Tute respects everyone's right to privacy and takes measures to ensure that all information is handled with care and respect. |
| **Safer Recruitment Policy:** | Sensitive personal data will be securely stored and will remain confidential. |

**Related documents:**

Appendix 1 - ICO Training Checklist for small & medium sized organisations

Appendix 2 - Email PrivacyConsiderations
Appendix 3 - Records Management Service retention guidelines for schools
Appendix 4 - Personal data security breach log

**References:**

Data Protection Act 1998
Information Commissioners Office (ICO)

**Resources:**

http://ico.org.uk/for_organisations/sector_guides/education

ICO Report on data protection guidance given to schools 2012

**Policy approved by:** Chris Baldock, CEO
**Date of last review:** 1st December 18