# ICT ACCEPTABLE USE POLICY | ICT-P-1

## 1. PURPOSE

1.1 The purpose of this Policy is to ensure that all devices and systems are used in line with expectations of the organisation with the aim to keep users and data safe and secure.

1.2 Technology is now entwined in our modern lives, with everyday use of social media and web-based communication a standard practice. It is therefore important to ensure good awareness both of the possibilities to learn, create, and share ideas, and also the risks that these freedoms bring both to the welfare of colleagues and students and to the integrity of the ICT systems that the school relies on to provide learning and teaching.

1.3 All users accessing our school systems are entitled to safe access to the internet and IT systems at all times.

1.4 This policy is outlines a working framework for colleagues to uphold the positive ideals of the technology we use while providing a safe learning environment and protecting the data we manage in the course of our services to students and their families.

1.5 This is not an exhaustive list, and all colleagues are reminded that ICT use should be consistent with the organisation's ethos, GDPR regulations, other appropriate policies, relevant national and local guidance and expectations, and the Law.

## 2. SCOPE

2.1 This Policy applies to:

(a) Indie Education (**Indie**) employees (including full time, part time, permanent, fixed term and casual), volunteers, and SCITT trainees.

(b) Information assets, whatever format, device or medium they are held in.

(c) All Indie Education owned information, in whatever format, wherever it is held (e.g. by a third party) for which Indie Education is the data controller.

## 3. RESPONSIBILITIES

3.1 Indie colleagues must:

(a) Understand that Information Systems and ICT include networks, data, and data storage, as well as both online and offline communication technologies and access devices.

- Examples include laptops, mobile phones, tablets, digital cameras, email, and social media sites.

(b) Ensure Indie Education owned information systems are used appropriately.

- The Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify

computer material without authorisation.

(c) Understand that any hardware and software provided by my workplace for staff use can only be used by members of staff. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I will not transfer organisational data to personal devices.

(d) Respect system security and I will not disclose any password or security information. I will use a 'strong' password (following organisation policies) and will not store this password in an insecure location. Where possible I will always use Multi Factor authentication as an additional security measure. It is recommended that you use a password manager such as Nordpass or Proton Pass (Free)...there are many others.

(e) Not attempt to install any purchased or downloaded software or hardware without permission from line manager and the CEO.

(f) Ensure that any personal data of learners, staff or parents/carers is kept in accordance with the General Data Protection Regulation (GDPR). This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary, and will be kept private and secure with appropriate security measures in place. Any data which is being removed from a college site's (such as email) will be encrypted by a method approved by out IT service support team. Any images or videos of pupils will only be used in line with Indie Education policy guidance and will always consider parental consent before processing. All Indie Education data must stay on organisation owned devices and never be transferred to personal devices.

(g) Not keep professional documents which contain organisation-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). If I choose to access Indie Education email system on my mobile device (tablet or mobile phone), the device must be pin, or password protected. I will protect the devices in my care from unapproved access or theft. Indie Education block access to organisation data from outside of the UK by default and only in some circumstances shall this be allowed.

- Personal data kept on work devices must be kept to a minimum (examples that do not meet this include filling the hard drive with music files or personal photos). I will ensure that I regularly cleanse data from my device/OneDrive to reduce unnecessary storage.

(h) Respect copyright and intellectual property rights including but not limited to the use of copyrighted images.

(i) Have read and understood the Social Media policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

(j) Have carried out Data Protection and GDPR training via appropriate programmes and am

confident in my understanding.

(k) Have read and understood the Mobile Phone and Loaned Property Equipment policy that covers the use of any phone/loaned equipment that I may have been provided to carry out my work.

(l) Report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (online safety DSL) and line lead as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the online safety DSL and your line manager.

(m) Not attempt to bypass any filtering and/or security systems put in place by the Indie Education. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to ICT services as soon as possible.

(n) Report any actual or potential data breaches to the Local Data Protection Representatives within 24 hours of the incident. The LDPR will upload data breaches to our GDPR records in TEAMs.

(o) Understand that Office 365 mailboxes (email) are not a storage system, and that Indie Education has a policy in place to delete emails after 3 years. Emails that are required beyond this put need to be saved outside of mailboxes.

- Electronic communications with learners, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will always be transparent and open to scrutiny. All communication will take place via approved communication channels e.g. via a provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking.

(p) Ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using Indie or personal systems. This includes, but not limited to, the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the organisations this policy (AUP) and the Law.

(q) Not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the organisation I work for into disrepute.

(r) Promote online safety and will help colleagues and our learners to develop a responsible attitude to safety online, system use and to the content they access or create.

(s) Understand that my use of the information systems, internet and email may be monitored and recorded to ensure policy compliance. This includes the use of monitoring software on all colleague's member's devices.

- Any personal device will only ever be connected to the Indie guest wireless network communicated by the IT service team.

(t) Understand that the use of USB storage devices is prohibited and agree not to use them.

(u) Understand the appropriate use of live webcams and online chat software where remote teaching and learning is required.

(v) Accept that use of 1:1 conference calls or chats, either colleague to learner or learner to learner is prohibited and groups of learners must only be organised by the teacher or adult leading the session.

(w) Ensure they uphold suitable clothing requirements (no PJ's or offensive slogan T-shirts) and that suitable clothing is worn by learners, as well as other household members, where they are likely appear in the background while webcams are switched on

- It will be the adult's responsibility to immediately switch off any webcams or remove a learners account from the group if the learner or their household member is wearing inappropriate or unsuitable clothing.

(x) Ensure that any devices are used in appropriate areas, for example, not in bedrooms; and that a neutral background is shown where possible (to avoid the endorsement of use of consumer products).

  - The blurring of backgrounds tool will always be used wherever possible, however, it will be the adult's responsibility to immediately switch off any webcams or remove a learners account from the group, if they feel the room being seen was inappropriate.

(y) Be responsible for ensuring that the live class is recorded and backed up elsewhere, so that if any issues were to arise, the video can be reviewed.

- Any safeguarding concerns seen or heard will be recorded on Arbor and reported to the online safety DSL immediately.

(z) Make sure that live sessions are kept to a reasonable length of time, as the streaming may prevent the family from 'getting on' with their day.

- The time-of-day live classes are timetabled will always fall within normal college hours.

(aa) Ensure that they use appropriate and professional language and that appropriate language is used by learners and their other household members, during sessions.

- Inappropriate language used by learners or heard by members of their household will be challenged and accounts will be muted, if necessary, by the adult.

(bb) Ensure that webcams and chat platforms are used for work purposes only and subject to the code of conduct standards set out in the Indie Education staff handbook and behaviour policy.

- A breach of these standards may result in disciplinary action.

(cc) Make a risk assessment of any AI platform before entering any colleague or student personal data and ensure that age limit guidance is followed when using generative AI tools. I.e., Copilot age limit guidance is 16.

## 4. POLICY REVIEW

4.1 In accordance with Indie's policy review protocol, this Policy will be reviewed annually. If there are material changes to circumstances before the 12-month review period, this Policy will be reviewed immediately to ensure its contents remain effective and up to date.

## 5. RELATED DOCUMENTS

- Indie Education Handbook
- Social Media Policy
- Data Protection Policy
- DfE guidance note and advice
- Document retention Management Policy
- Whistle blowing Policy
- Related Legislation
- Behaviour Policy
- Mobile Phone Policy

## 6. AUTHORISATION

6.1 This document has been authorised by the Chief Executive Officer.

## ICT ACCEPTABLE USE POLICY – EMPLOYEE DECLARATION

I ……. declare that I have read and understood the contents of this ICT Acceptable Use Policy and my responsibilities as set out within.

Additionally, I confirm my understanding that this forms part of the terms and conditions as set out in my contract of employment and that failure to adhere to this policy may result in disciplinary action.

| | |
|---|---|
| Signed: | |
| Print Name: | |
| Date: | |