Jus'T'Learn
Independent School

Jus'T'Learn Independent School
9-11 Commonside East, CR4 2QA
020 8648 9662 / 07415 368 981
Email - info@justlearn.org.uk
www.justlearn.org.uk

Jus'T'Learn

ICT E-Safety Policy

Autumn 2013

Review date: Autumn 2014 – No amendments made

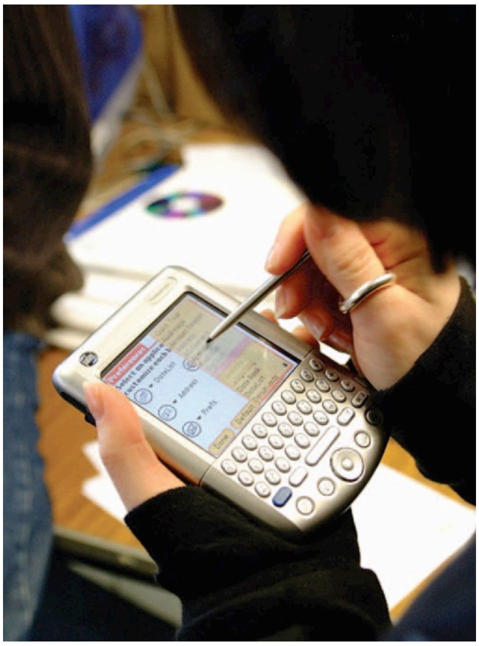
Review date: Autumn 2015 – No amendments made

Review date: Spring 2017 – Changes to the words from Centre Head to Head of school and removed floppy disk.

Review date: Spring 2018 – Changes made to the transferring of information. New GDPR guidelines, May 2018.

Review Date: Spring 2019

Contents



1. An overview of the risks

ICT can offer many positive educational and social benefits to young people, but unfortunately there are some dangers. Some young people may find themselves involved in activities which are inappropriate, or possibly illegal. Some of the issues and risks are summarised below.

Jus'T'Learn has technologies in place to restrict inappropriate access, but it must be borne in mind that pupils may bring an increasingly sophisticated range of handheld devices into school giving them separate access to potentially unsuitable materials.

Jus'T'Learn is governed and monitored by our IT providers called Liquid IT which has put in place secure blocking. Jus'T'Learn has blocked certain internet access, email and chat services, social networks so that our pupils may not be exposed to inappropriate material.

Copyright infringement

Copyright law applies on the internet, but is ignored by many young people who download and swap music files, cut and paste homework assignments from others' work, or even purchase whole assignments from online cheat sites without realising the implications and consequences.

Inappropriate or illegal behaviour

Our pupils may get involved in inappropriate, antisocial or illegal behaviour while using new technologies. Just as in the real world, groups or cliques can form online, and activities that start out as harmless fun, such as voicing an opposing opinion to another member of a chat room, can quickly escalate to something much more serious. Jus'T'Learn takes a serious view of any form of bullying and due to the advent of new technologies this unfortunate aspect of their use can be used by our pupils.

2. The importance of ensuring a safe ICT learning environment

Jus'T'Learn wants to create a safe ICT learning environment. Liquid IT has developed technological tool which is very effective and is a comprehensive internet safety programme, as outlined below:

• an infrastructure of whole-school awareness, designated responsibilities, policies and procedures

• an effective range of technological tools

• a comprehensive internet safety education programme for the whole school community.

To be truly effective, Jus'T'Learn internet safety policy is regularly reviewed by the Head of School and ICT teacher, considering new and emerging technologies and changes in local circumstances. Jus'T'Learn internet safety policies should be embedded within a cycle of establishment, maintenance, ongoing review, modification, reporting and annual review, supported by technological solutions wherever possible.

An effective range of technological tools

There are a number of technological tools that Jus'T'Learn can employ to safeguard both pupils and the system itself:
• A firewall and virus protection.
• Monitoring systems - to keep track of who downloaded what, when they downloaded it, and using which computer.
• Filtering and content control – to minimise access to inappropriate content via the school network.
There are a range of products to help in these processes and the choice is likely to depend on the school's type, size, in-house technical expertise and budget.

3. Whole-school responsibilities for internet safety

Internet safety must be a whole-school responsibility. The Head of School has overall responsibility for the day-to-day administration and management of the school. The network manager has an important role to play in establishing and maintaining a safe ICT learning environment for the school, and will be a key member of the school's internet safety team. The ICT teacher is responsible for the internet safety within the class room.

The network manager is responsible for:

• acting as a key member of the school's internet safety team, supporting the internet safety co-ordinator in the development and maintenance of appropriate policies and procedures through technical information and advice

• providing a technical infrastructure to support internet safety practices; this might include:
• ensuring that appropriate and effective electronic security systems are in place, such as filtering, monitoring and firewall technology, and virus protection supported by regular and thorough monitoring of computer networks
• reporting network breaches of acceptable use of ICT facilities to the internet safety co-ordinator and other staff members as appropriate
• a member of SLT is responsible for the overall maintenance of Internet safety

The ICT teacher will be responsible for:
• developing additional internet safety policies where necessary within the subject area/department. A departmental policy should outline the importance of embedding internet safety messages within the context of the curriculum – and Signposts to Safety (for Key Stages 3 and 4)
• the departmental policy should also consider what safety measures are appropriate for a particular situation (for example in the ICT suite or in the classroom), and the specific technologies used within the teaching of the subject.
• developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children and young people
• ensuring any instances of ICT misuse, whether accidental or deliberate, are dealt with through the proper channels, reporting to the internet safety co-ordinator in line with school internet safety policies
• ensuring that pupils who experience problems when using the internet are appropriately supported, working with the internet safety co-ordinator as appropriate.

Classroom teachers and teaching assistants
The responsibilities for classroom staff include:
• developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children and young people
• implementing school and departmental internet safety policies through effective classroom practice
• ensuring any instances of ICT misuse, whether accidental or deliberate, are dealt with through the proper channels, reporting to the internet safety co-ordinator in line with school internet safety policies
• ensuring that they provide the necessary support to pupils who experience problems when using the internet, working with the internet safety co-ordinator, pastoral teams and/or child protection liaison officers as appropriate
• planning classroom use of the internet and ICT facilities to ensure that internet safety is not compromised; for example, evaluating websites in advance of classroom use (for example, by book marking and caching sites) and ensuring that school filtering levels provide appropriate protection for topics being studied
• embedding teaching of internet safety messages within curriculum areas wherever possible
• maintaining an appropriate level of professional conduct in their own internet use both within and outside school.

Pupils

The responsibilities of the pupils themselves in creating a safe ICT learning environment should not be underestimated. Pupils should be encouraged to contribute to the creation of

school policies, with pupil representation on the school's internet safety policy team and involvement in developing classroom rules and internet safety resources. Through this approach, pupils will develop a greater understanding of the issues involved, and will feel more ownership of and accountability for the policies.

The ultimate aim is for pupils to take responsibility for their own actions when using the internet and other communications technologies, with each pupil developing a set of safe and discriminating behaviours to guide their own internet use. Pupils should develop confidence in their own abilities, but should also recognise when it is appropriate to seek help and advice, and know where such help can be found. Pupils should also take a responsibility for talking to their parents or carers about internet safety issues, working with them to develop a set of rules for safe internet use in the home.

Specific responsibilities for pupils might include:

• contributing to school internet safety and acceptable use policies through involvement in the school's internet safety policy team

• upholding school policies relating to acceptable use of the internet and other communications technologies

• developing their own set of safe and discriminating behaviours to guide them whenever they are online

• reporting any incidents of ICT misuse within school to a member of the teaching staff

• seeking help or advice from a teacher or trusted adult if they experience problems when online, or if they receive any content or contact which makes them feel uncomfortable in any way

• communicating with their parents or carers about internet safety issues, and upholding any rules for safe internet use in the home.

4. Internet safety in the classroom

Education on internet safety issues is essential – although there are many powerful benefits to the use of the internet and communications technologies, this new environment can present very real and serious risks for the uninformed, the unwary and the unwise. Children and young people, whom society has a duty to protect, may be the ones most at risk.

It is important that teachers, parents and carers do not confuse skilful use of new technologies with an ability to perceive and avoid risk – internet and ICT literacy is unfortunately not synonymous with internet and ICT safety.

Schools have a responsibility to educate young people and provide a safe learning environment. Increasingly, ICT is used as an integral part of teaching and learning, and evidence shows that it can have many important benefits. Schools, therefore, must also play a special role in educating children and young people about safe use of the internet and related technologies. Classroom teachers and teaching assistants will be instrumental in this process. Careful consideration should be given to where and when internet safety education takes place. While discrete lessons are useful, internet safety concepts should be embedded within the curriculum wherever possible, while safety messages should be reinforced every time pupils use the internet and related technologies. Classroom staff should work together with their subject co-ordinators or heads of department, to ensure that a comprehensive, consistent and continuing programme of internet safety education takes place across subjects, year groups and throughout the school.

5. Responding to incidents of misuse

Development in this area needs to occur, with SLT taking the lead. The Centre Head should lead on this issue and will take the appropriate actions.

6. Storage of Digital Portable Devices in the Classroom

Classroom remote digital device introduces vulnerabilities such as losing the device, theft, breakage of the ICT and media devices. The nature of portable ICT devices and media increases the risk to the information stored on them due again to the increased chance of loss or theft compared to fixed devices. All devices will require an individual code, with a signing in and out procedure completed by the Learning Mentor who will log the items supplied to individual staff and the appearance of the device this is in case the device is tampered with.

Prior to the implementation of the portable digital devices in the rooms an in-depth risk assessment will be required with the view points of the device supplier providing support and training where required to members of staff.

If a member of staff needs to leave their desk/room unattended the staff member should ensure that digital device is locked away and secured, keys to draws/cabinets should be provided. Keys to all draws/cabinets should be made available with a replacement key kept locked away and only designated persons (Business Manager and The Head of School) should have access to the keys. Again a record of monitoring the placement of the keys should be kept with the Technician.

Due to the sensitivity of the device, extra vigilance should be undertaken by the staff. The device should be placed in an area where pupils are unable to access the item, or a cover will need to be placed on the computer to ensure that the device is not taken. Any loss, theft or damage to any of the devices must be reported to the Technician immediately**.**

7. Use of e-mail

The e-mail system is the property of Jus‘T’Learn and all copies of messages created, sent, received or stored on the system are and remain the property of Jus‘T’Learn. Such messages are not the private property of any individual nor shall any individual expect there to be any personal privacy with respect to any such message, whether it be designated “private” or not.

Jus‘T’Learn maintains the right to review, audit, intercept, access, monitor, delete and disclose all messages, including attachments, created, sent, received or stored on the e-mail system for any purpose. Use of Jus‘T’Learn’s e-mail system by a staff implies that the staff recognises and consents to the rights of Jus‘T’Learn described above.

Jus‘T’Learn maintains its e-mail system solely for business use. The use of the e-mail system for any other purpose is a violation of the school’s policy. Unauthorised activities include, but are not limited to:

- The transmission or storage of offensive material which is of a sexual or pornographic nature
- The transmission or storage of messages containing sexual implication, racial slurs, gender-specific comments, defamatory statements, or any comments denigrating a person’s age, sexual orientation, religious or political beliefs, national origin or disability
- The transmission or storage of materials that infringe copyright or intellectual property rights of any third parties
- Engaging in improper or illegal activities

8. Security of Information

The objective of information security is to ensure the schools continuity and minimise damage by preventing and minimising the impact of security incidents. Jus‘T’Learn is committed to the secure keeping of all the school’s information assets from all threats, whether internal or external, deliberate or accidental. This includes the information stored on its computers, transmitted across its networks, printed out or written down on paper, stored on disk, sent by fax or spoken in conversation and over the telephone.

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing ‘privacy notices’ (sometimes called ‘fair processing notices’) to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils**.

We, Just Learn Independent School, are the ‘data controller’ for the purposes of data protection law.

Our data protection officer is Mrs Zarah Jussab-Gadatara

How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. As a school we follow the Information and Records Management Society's toolkit for schools regarding how long we keep information about pupils. Please refer to:

https://c.ymcdn.com/sites/irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf

Data sharing

We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- *Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions*
- *The Department for Education*
- *The pupil's family and representatives*
- *Educators and examining bodies*
- *Our regulator [specify as appropriate, e.g. Ofsted, Independent Schools Inspectorate]*
- *Suppliers and service providers – to enable them to provide the service we have contracted them for*
- *Financial organisations*
- *Central and local government*
- *Our auditors*
- *Survey and research organisations*
- *Health authorities*
- *Security organisations*
- *Health and social welfare organisations*
- *Professional advisers and consultants*
- *Charities and voluntary organisations*
- *Police forces, courts, tribunals*
- *Professional bodies*

Appendix 1:

ICT POLICY DOCUMENTS

1. I have read and understood the Policy Documents set out above and agree to abide by the Policies and Procedures as specified.

2. I understand that Internet access and E-mails will be intercepted, monitored and read in order to ensure that the content is in accordance with the Jus'T'Learn Policy.

Staff Sign: ___________________________ Date: ______________________________

(Print Name): _________________________ Department: _________________________

Manager Sign: ________________________ Date: ______________________________