> “Before you become too entranced with gorgeous gadgets and mesmerizing video displays, let me remind you that information is not knowledge, knowledge is not wisdom, and wisdom is not foresight. Each grows out of the other, and we need them all.”
>
> **Arthur C. Clarke**

INTERNET AND COMMUNCATION TECHNOLOGY POLICY

The use of technologies at home and school can bring great benefits, provided it is appropriately managed and is flexible in the face of constantly evolving online potential dangers – thus ensuring appropriate, effective and safe use of Information, Communication and Technology.

The internet being an essential element for children and adults in 21st Century life, for education, business and social interaction, J&R Care Ltd have a duty to provide residents and pupils with quality and safe internet access as part of their learning and development.

Children will use the internet widely when outside of the home and at school and will need to learn how to evaluate internet information and to also help take care of their own safety and security.

J&R Care Ltd and The Annex School recognise the risks of allowing children and staff to use the internet and are pro-active in continued ICT education.

The Joys of Technology

Whereas some people may regard the above heading with a degree of scepticism, the school's ICT teacher is very enthusiastic about technology. Having programmed his first computer in 1981 when he was 9 years of age, he now works in industry as a Technology Support Specialist and ICT Consultant. ICT education for young people he believes is so vital, and sadly lacking in wider society, he is glad to teach ICT.

In his line of work he meet all sorts of people using computers and technologies, of all ages and levels of technological ability and familiarity. Technology is everywhere in 21st Century life, and he affirms that support from the high street, friends or family, is either non-existent, impersonal, insufficient or just doesn't actually help at all.

We believe technology should be used and enjoyed safely and productively at work and play, and therefore at least a modicum of ICT knowledge is essential for everyone.

If ICT learning at The Annex School sparks their interest and they go on to study the subject in-depth, expectations will have been wonderfully exceeded. At the very least, we want them to gain a good basic ICT knowledge which will allow them to continue enjoy using information, communication and technology effectively and safely.

Strategy

- Discover individual pupil's wider interests
- Assess ICT technical ability
- Work through the European Computer Driving License (ECDL) and collate a body of work supporting their progress
- Tailor tasks to their level of understanding and their interests (i.e. sport, gaming or music)
- Try and spark an interest or greater in the world of technology

Methods

- Moving between and spending time with each pupil in a teacher / support manner
- Bespoke tasks pertaining to each pupil's level of understanding
- Being flexible and able to quickly adapt tasks – i.e. increase number of tasks or it is evident they are struggling because it is too easy or too difficult
- ICT Points. Each task has a set amount of points attached to it, and pupils receive ICT Points if they complete all the tasks. If they do not get all the points they are shown why. They can then redo the task the tasks following week(s) to get the points they missed.
- Different tasks take into account each pupils level of understanding and the fact that different children work at their own pace. Less complicated tasks for pupils who are not as advanced as older children will receive the same amount of points, based on the bespoke tasks, effort and effort.
- A running total of ICT Points is on the classroom wall.

ICT points are made inclusive, fun, and healthy competition, with rewards at the end of the year and a Digital Champion Award.

NB. ICT Points are separate from school behavioural points

ICT Lesson Content

Pupils can use a number of different applications in the line of their school work, including Microsoft Office, Paint Shop Pro, Python and Scratch.

Teaching them how to use software effectively in the world of education also helps them prepare for computer use when they enter the wider world, and part of ICT lessons focus on the European Computer Driving License (ECDL) syllabus, which consists of:

1. Concepts of ICT
2. Using Computers and Managing Files
3. Word Processing
4. Spreadsheets
5. Using Databases
6. Presentation
7. Web Browsing and Communication

It is not sufficient though to just learn the ECDL. Pupils who are also taught basic programming, specifically Python and HTML (Hyper Text Markup Language – the computer language at the foundation of the World Wide Web).

Younger children are taught to use Scratch programming which teaches pupils in a fun way the basic algorithmic principals of any computer programming language.

Keeping children focussed and interested in all areas is essential, and being creative with how lessons are taught includes quizzes, bespoke ICT crosswords and word searches (course/task specific), discussion, PowerPoint presentations, computer history, YouTube film clips (for analogies prior to lesson commencement), and tasks that involve subjects that interest them like music, sport, cars and gaming.

Differentiated Learning

With pupils of different ages and having attained different levels of computer knowledge and experience, it is important to:

> **a)** not teach subject matter that is too easy or for no reason repeatedly go over ground already covered
> **b)** not teach subject matter that is beyond their level of understanding
> **c)** allow pupils to go at their own pace while continuing to patiently nudge them forward

To facilitate the above it is necessary to teach by moving amongst the pupils in a teacher / support manner. With lessons and tasks pre-planned and printed, the LSA and other staff can help keep everyone on track.

A new pupil's level of understanding can be assessed over 2 lessons. First they are given ICT Functional Skills questions. If they pass they are given multiple choice quizzes on ICT Concepts and, depending on their level of understanding, they are asked to create Word or Excel document, and to even (if their abilities allow) submit a 10 page PowerPoint presentation on their favourite subject.

If attention span or behavioural issues are an issue, the assessment may require additional lessons or an individual approach to be tailored in order to get them engaged in the subject.

Finding out about their interests is one way [i.e. football, video games or music), or sometimes it is necessary to step back, keep them included in the lesson and help them make a start and encourage them.

Lesson subjects can also be introduced to all pupils at once, and then ICT teacher sets pre-determined tasks appropriate to a pupil's level of understanding, moving between pupils in a teacher / support manner.

World Wide Web

Web browsing filters and computer system restrictions are in place on all computers and devices. Prohibited websites are also blocked via the router.

The DNS servers are also made more secure by using opendns.com.

Pupils are also taught about computer security and how to keep safe online, both practically and .

Online Gaming

Gaming can be great fun and is a place where children play. There are however risks with online multiplayer games, and these are not permitted during free time at the school. They aren't permitted at the house either, they are blocked.

Security

While smart and tech savvy children can be adept at bypassing security or attempting to, spot checks and overseeing their activity is always in place, and sanctions on technology access is strictly enforced if checks reveal breaches of the school's security policy.

Photography by staff or pupils is not permitted, except with express permission and is overseen by the teacher.

Pupils may not bring smartphones to school.

Staff will have smartphones switched to silent and kept locked in the office, or securely about their person. Nevertheless, PIN secured screen-locks must be activated and on no account must a pupil be aware of it.

Online Dangers

Despite close attention by staff, quick children are adept at ‘slipping underneath the radar’. The risks and dangers inherent in the online world are explained to all pupils, even though some pupils may roll their eyes at this kind of talk. That is why they are taught about the ever evolving online dangers, even though they might think that they already know.

The biggest risk can arise when children give out their personal details to strangers. The online world can often seem very different to the real world for children, and they can be tempted to say and do things that they wouldn't dream of if they met someone face to face. This can include giving out personal information such as mobile numbers and pictures of themselves. If they are talking to another child there is a risk that they will misuse this information - for example, by texting abusive messages to the child, or by posting their image on a website; but there is obviously a greater risk if the person that they are chatting to is an adult. Unfortunately, paedophiles - adults who want to meet children for sex - use the internet, often with the intention of talking with and meeting a child. Children can be naive to this risk, and often feel that they are invincible, or that 'they would know if someone was lying'.

Child sex abusers find the internet an easier place to participate in a range of child sexual abuse activity including contact with children due to the anonymity of the medium. They will often lie and pretend to be younger than they are or people other than themselves, and find a sense of security by operating from the safety of their own homes. They have been known to set up bogus email accounts and chat personas to mask their identity online

There are a number of actions which these adults will engage in online. These include:

- Swapping child abuse images in chat areas or through instant messenger with other adults or children and forming networks with other child abusers to share tips on how to groom more effectively and how to avoid being caught.
- Swapping personal information of children that they have collected with other abusers
- Participating in online communities such as blogs, forums and chat rooms with the intention to groom children, collect sexually explicit images and meet them to have sex.
- Online Grooming is: "A course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes."

Often, adults who want to engage children in sexual acts, or talk to them for sexual gratification will seek out children who desire friendship. They will often use a number of grooming techniques including building trust with the child through lying, creating different personas and then attempting to engage the child in more intimate forms of communication including compromising a child with the use of images and webcams. Child sex abusers will often use blackmail and guilt as methods of securing a meeting with the child.

General Policy Provisions

J&R Care Ltd are committed to ensuring children's safety online and have developed a policy on its use in the home and school:

Our internet safety policy has been written by the directors of the company, building on the Kent County Council's e-safety policy and guidance.

J&R Care Ltd has an Internet Safety Officer who will ensure that:

- The home/school internet access is designed expressively for residents/pupils use and will include filtering appropriate to the children's age and understanding.
- Residents will be taught what internet use is acceptable and what is not and given clear objectives for its use.
- The computers in the home/school have been positioned in all areas to allow easy supervision of the work/content being displayed and hence discourages breaches of acceptable use.
- Staff will guide the child in online activities that will support the learning and development planned for the child's age and maturity.
- No child will have access to the internet without consultation with a member of staff and the access will be supervised and monitored.
- The company and its staff will ensure that the copying and subsequent use of the internet complies with copyright law.
- The security of the homes/schools computer will be inspected and updated every six months.
- Virus protection is regularly updated.
- Portable media may not be used without specific permission by the Internet Safety

The School's dedicated Data Protection Officer conducts regular security checks on all systems.

- Files, web sites and emails on the homes/schools network will be regularly checked and monitored.
- Children and Staff may only use approved email accounts.
- A central email address for staff
- Access in the home/school to personal email accounts is prohibited by both staff and children. Email sent to external organizations should be written carefully and authorized by a senior member of staff before sending.
- The forwarding of chain letters is not permitted.
- No resident /pupil or staff member will be authorized to place photos on any social network space.
- The use of web cams in the home/school is strictly prohibited, unless for specific supervised pieces of work within the school.
- Emerging technologies will be examined for educational/social development benefit and a risk assessment will be carried out before use in the home/ school.
- The home school will maintain a current record of all staff and residents activity online and will be signed by the manager of the home and stored in the main office.
- Social workers/parents will be asked to sign a consent form for resident's access in the home.
- An e-safety training programme will be introduced to raise awareness of the importance of safe and responsible internet use.
- Staff and children will be asked to sign an internet code of conduct before being allowed to use the internet.
- The use of the computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990
- Complaints of internet misuse will be dealt with by the Internet Safety Officer and the Directors and discussions will be held with the local police to establish procedures for handling potential illegal issues.
- Consequences within the home for misuse of the computers/internet will include: Investigation by the ISO/directors; informing social workers/parents; removal of the internet or computer access for a period of time.
- Staff who misuse the computer/internet will be dealt with through the companies disciplinary procedure
- Any staff member found to be interfering or deleting any monitoring system will be dealt with through the companies' disciplinary procedure.

All staff will familiarise themselves with legal documentation relevant to internet safety, use and abuse, which include:

- The Sexual Offences Act 2003 , which introduces new offences of grooming and in relation to making/distributing indecent images of children, raised the age of the child to 18 years old.
- The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds.
- The Police and Justice Act which extended the reach of the computer misuse Act 1990 making denial of service attacks a criminal offence.
- Communications Act 2003 (Section 127)
- Data Protection Act 1998 (Sections 1-3)
- Malicious Communications Act 1988 (Section 1)
- Copyright, Design and Patients Act 1988
- Public Order Act 1986 (Sections 17-29)
- Protection of Children Act 1978 (Section 1)
- Obscene Publications Act 1959 and 1964
- Protection from Harassment Act 1997
- Regulation of Investigatory Powers Act 2000
- The Telecommunications (lawful business practice)(Interception of Communications) Regulations 2000

Mobile phones

Whilst J&R Care Ltd will tolerate staff using mobile phones for essential calls during working hours (i.e. if on an outing and a work mobile is not available), personal calls for staff and pupils are prohibited during lessons.

Also prohibited are casual chats, text messaging, e-mailing web, browsing and the taking of video and/or still images. Phones should be set to a silent ring during working hours. If staff wish to use a mobile phone they are requested to do so by first seeking permission from a Manager.

No pupil should bring a mobile phone to school. If a mobile phone is brought into the classroom, the teacher will ask that it is handed over to them. If the child refuses, they will be asked to leave the room and technology use sanctions may be used.

Updated May 2018