NovaCity Centre

NovaCity Centre, Unit 1: The Summit, Mangham Road, Rotherham, S61 4RJ

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Our e-Safety Policy has been written by NovaCity. It has been agreed and approved by the board of directors

The e-Safety Policy will be reviewed annually. During the January Audit of Policies and Procedures

Why is Internet Use Important?

The purpose of Internet use within NovaCity is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the Companys' management information and administration systems.

Internet use is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for participants who show a responsible and mature approach to its use. NovaCity does not have to provide participants with quality Internet access but understands its positive outcomes when used.

Participants will use the Internet outside of NovaCity and will need to learn how to evaluate Internet information and to take care of their own safety and security. NovaCity is not directly responsible for this but will endeavor to provide guidelines and advice where necessary and appropriate

Authorised Internet Access

- Wifi and internet access is strictly controlled within NovaCity Premises and not publicly available apart from designated, supervised machines.

World Wide Web

- If any user discovers unsuitable sites, the URL (address), time, content is reported to the Local Authority via the centre manager
- NovaCity ensures that the use of Internet derived materials by users complies with copyright law.
- Users are taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Staff Internet Usage

- Whilst using NovaCity's internet on privately owned computers staff are expected to be responsible in its usage
- Staff are encouraged to be responsible whilst using social media, email and the internet via their own devices.
- Staff appliances are not to be given to users of the centre under any circumstances.
- Using the internet as an aid to business is quite apparent. The use of social media tools as advertising methods is not to be overlooked as a valuable resource. Restricting access to video sites (youtube), social media (facebook) and email is to restrict the functionality of the business. It is therefore reasonably acceptable under general circumstances for this activity to occur in private, locked offices and on personal appliances such as smart phones and laptops whilst with NovaCity premises.

User Internet Usage

- Access to wifi as a method to connect to the internet is prohibited.
- Users must always use wired PC computers in the computer suite
- Access to the computer suite is controlled and supervised
- Filters are present to ensure access to unwanted content is restricted.
- Users are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others.

Mobile Phones

- Mobile phones are allowed in the building and are encouraged to be used unless it is at the detriment to the activities taking place. Young people should be encouraged but educated on safely sharing their experiences with family and friends whilst using the centre.
- When cameras are used by staff to take pictures of classes they are stored securely and or deleted when there is no use for them. (Removed from personal devices immediately.) This is made clear on the entrants form that all users must sign before entry to the building. If photos or videos cannot be taken of a young person this needs to be brought to the attention of the training team.

Published Content and the School Web Site

- The contact details on the Web site will be the school address, e-mail and telephone number. Staff or participants personal information will not be published.

Publishing Users Images and Work

- Photographs and video that include users will be selected with direct permission from parent or guardian

- The act of sharing users content on company media will be allowed after vetting the media for inappropriate content. Such media should be used to inspire other to share and interact positively with the content.

Information System Security

- NovaCity ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Assessing Risks

- NovaCity will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a NovaCity computer. NovaCity cannot accept liability for the material accessed, or any consequences of Internet access.
- NovaCity will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling e-safety Complaints

- Complaints of Internet misuse are dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Manager.
- Complaints of a child protection nature must be dealt with in accordance with NovaCity child protection procedures.
- Users will be informed of the complaints procedure.

Communication of Policy

Users

- Rules for Internet access will be posted in all networked rooms.
- Users will be informed that Internet use will be monitored.

Staff

- All staff will be given the NovaCity e-Safety Policy and its importance explained.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Appendix **A**

eSafety Incident Log

Date of incident:	
Member of staff reporting incident:	
URL, (web address) of incident:	
Copy of screens/evidence saved to:	
Location of incident (room):	
Computer number if known:	
Details:	
Passed to:	
Action taken	

)

Appendix **B**

Current Legislation

Acts relating to monitoring of individuals

Data Protection Act 1998
The Act requires anyone who handles personal information to comply with 8 important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIPA was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
The Act is one of the most significant pieces of constitutional legislation enacted in the United Kingdom. It is a key part of the Government's programme to encourage a modern civic society where the rights and responsibilities of our citizens are clearly recognised and properly balanced. Its effect is to allow people to claim their rights under the European Convention on Human Rights in UK courts and tribunals, instead of having to go to the European Court in Strasbourg. The Act underpins this by requiring all public authorities in the UK to act compatibly with the Convention rights. This places new responsibilities on all of us who work in public authorities, which includes central government, the courts, the Police, local government and many bodies who carry out functions which the Government would otherwise have to undertake.

http://www.justice.gov.uk/guidance/humanrights.htm

Other Acts relating to eSafety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.
http://www.opsi.gov.uk/acts/acts2006/ukpga_20060001_en_1

Public Order Act 1986 (sections 17– 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.
http://www.opsi.gov.uk/acts/acts1986/pdf/ukpga_19860064_en.pdf

Crime and Disorder Act 1998
The Crime and Disorder Act 1998 promotes the practice of partnership working to reduce crime and disorder and places a statutory duty on Police and Local Authorities to develop and implement a strategy to tackle problems in their area. In doing so, the responsible authorities are required to work in partnership with a range of other local public, private, community and voluntary groups and with the community itself.
The Acts key areas were the introduction of Anti-Social Behaviour Orders (ASBO's), Sex Offender Orders, Parenting Orders and the introduction of law specific to 'racially aggravated' offences.
http://www.opsi.gov.uk/acts/acts1998/19980037.htm

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sex act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust.
Schools should already have a copy of "*Children & Families: Safer from sex Crime*" document as part of their child protection packs.
http://www.opsi.gov.uk/acts/acts2003/ukpga_20030042_en_1

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.
http://www.opsi.gov.uk/ACTS/acts2003/ukpga_20030021_en_13#pt2-ch1-pb20-l1g127

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:
- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.
http://www.opsi.gov.uk/acts/acts1990/ukpga_19900018_en_1#pb1-l1g1

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send a letter (including an email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.
http://www.opsi.gov.uk/ACTS/acts1988/Ukpga_19880027_en_1.htm

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.
http://www.copyrightservice.co.uk/copyright/p01_uk_copyright_law

Protection of Children Act 1978 (section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.
http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1978/cukpga_19780037_en_1

Obscene Publications Act 1959 and 1964
An Act to amend the law relating to the publication of obscene matter; to provide for the protection of literature; and to strengthen the law concerning pornography.
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.
http://www.statutelaw.gov.uk/content.aspx?LegType=All+Legislation&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&sortAlpha=0&PageNumber=0&NavFrom=0&parentActiveTextDocId=1128038&ActiveTextDocId=1128040&filesize=45334

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.
http://www.opsi.gov.uk/acts/acts1997/ukpga_19970040_en_1

Privacy and Electronic Communications (EC Directive) Regulations 2003 (Including spam)
The Privacy and Electronic Communications Regulations set out rules for people who wish to send you electronic direct marketing, for example, email and text messages.

http://www.ico.gov.uk/what_we_cover/privacy_and_electronic_communications/the_basics.aspx

Appendix **C**

Glossary

Some of the following phrases and acronyms are found within this policy. There are others that do not appear but may help to serve as a useful reference elsewhere:

API: Acronym for Application Program Interface, a set of tools, routines and rules for building software applications in a consistent way.

Asynchronous Learning: Mode of learning event in which participants are not online at the same time and are unable to communicate without time delay.

Authentication: Process of confirming the identity of an individual.

AUP: Acronym for Acceptable Use Policy i.e. agreed procedures in place to minimize eSecurity and eSafety risks.

AVI: Acronym for Audio Video Interleave - the file format used by Microsoft Video for Windows.

Bandwidth: Term that describes how much data can be sent via a connection in a specified time. This measurement is typically described in bps or bits per second.

Becta: British Educational Communications and Technology Agency - A Government funded agency promoting use of ICT.

Bit: The minimum unit of computer data - either a 0 or a 1.

Blog: A blog (a contraction of the term "web log") is a type of website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video.

Bps: Acronym for Bits per second the units in which the speed of modems are rated. Indicates the amount of information a modem can transmit and receive each second.

Browse: Process of viewing web pages over the World Wide Web.

Browser: Program that allows you to view and interact with web pages on the World Wide Web.

Byte: Unit for measuring data - usually 8 bits.

CEOP: The Child Exploitation and Online Protection Centre - delivers a multiagency service dedicated to tackling the exploitation of children.

CD: Acronym for Compact Disc. Originally an audio-only format the CD has spawned a range of derivatives including CD-ROM (Compact Disc Read Only
Memory), CDi (Compact Disc Interactive) CD-R (CD-ROM Recordable) and most recently CD-RW (Compact Disc Read Write).

Chat: Talking to one person or many people, usually in text format via the internet.

Childnet: A non-profit organisation working with others to help make the Internet a positive and safe place for children and young people.

Compression: Reducing the size of a file so that it can be transmitted more quickly and takes up less storage space.

Cookie: Small element of data sent to your computer when you visit a website. When you subsequently return to the site, this data may be used for a range of things including recalling your username.

DHTML: Acronym for Dynamic HTML - a new way of developing web pages with enhanced functionality. Standards for DHTML are still being developed.

Digital: Made up of zeros (0) and ones (1) or bits of information

DNS: Acronym for Domain Name System - the system that regulates naming of computers on the internet. The core of the system is a vast database that stores the names and network addresses of every computer, accessed whenever a computer needs to convert a Domain Name into a numeric IP address.

Domain: Official name for a computer attached to the Internet. Email addresses normally consist of a user ID and a domain name separated by the @ symbol.

Download: The process of copying files from one remote host to your computer, usually via FTP.

DVD: Acronym for Digital Versatile Disc.

eLearning: Wide range of electronic learning applications and processes including Web-based learning, computer-based learning, virtual classrooms and digital collaboration. Commonly held to include delivery of content via the Internet, intranet, extranet (LAN/ WAN), audio, video tape, satellite broadcast, interactive TV and CD-ROM.

eMail: Sending electronic messages over a network or the internet.

End user: The individual using ICT equipment at the time.

eSecurity: Procedures to ensure all electronic data is categorised as public, restricted or protected and that electronic systems containing the data are securely maintained.

eSafety: procedures to ensure computer users know their access rights and responsibilities in using ICT.

Extranet: A local area network (LAN) or wide area network (WAN) using HTML, SMTP, only available to people inside and certain people outside an organization, as determined by the organization.

FAQ: Acronym for Frequently Asked Questions.

Flash: A vector graphic animation tool marketed by Macromedia and widely used for developing web delivered e-learning.

FTP: Acronym for File Transfer Protocol. A process that allows you to transfer files or programmes to or from computers across the internet.

GIF: Acronym for Graphics Interchange Format - a common format for the storage of largely non-photographic imagery.

Gigabyte: 1024 megabytes of computer data.

Hardware: Physical technology such as computers, monitors and keyboards rather than software.

Hits: The number of requests for information made to a server.

Host: Computer that exists to allow other computers to connect with it.

HTML: Acronym for Hypertext Mark-up Language - the basic language that is used to construct web pages. There are several HTML standards in existence, the latest of which is HTML 4.

HTTP: Acronym for Hypertext Transfer Protocol, the standard that regulates the way information is transferred around the World Wide Web.

Hyperlink: Underlined word or set of words that, when clicked, takes you to a different place on that page or to a new destination altogether.

ICT: Acronym for Information and Communication Technology.

Internet: The full range of networks interconnected via internet protocol.

IP: Acronym for Internet Protocol, the rules that regulate the way information is transferred across the Internet.

IPS: Acronym for Intrusion Prevention System - a network security device that monitors network and/or system activities for malicious or unwanted behaviour and can react, in real-time, to block or prevent those activities.

ISP: Acronym for Internet Service Provider - companies that provide users with access to the internet.

Intranet: A private network inside an organisation that uses Internet technology, but is segregated from the Internet by a firewall. This means that authorised users can only access this network.

ISDN: Acronym for Integrated Services Digital Network. This telecommunications technology provides increased bandwidth using telephone lines but generates significant additional cost.

Java: Language developed specifically for creating software that can be simply downloaded from the Internet, but now used for a wide range of applications.

Javascript: Language similar to Java but actually incorporated into web pages in the interests of creating various special effects.

JPEG: Acronym for Joint Photographic Experts Group - the committee that originally developed this special image file format. JPEG files are now the most popular format for storing photographic images.

Kilobyte: Unit of computer data, made up of 1024 bytes.

Learning Platform: A Virtual Learning Environment (VLE) with facilities for communication, work storage and access to learning resources.

Learning Portal: A website that offers learners consolidated access to learning and training resources from multiple sources.

Login: The action involved in entering a computer system or the account name you have been authorised to gain access to a system with.

Megabyte: Unit of computer data made up of 1024 kilobytes.

MIS: Acronym for Management Information System - provides a co-ordinated approach to the gathering and use of data.

Modem: Device that allows one computer to connect to another via a telephone line.

MPEG: Acronym for Moving Picture Experts Group - the committee who devised this innovative file format for storing video images.

Network: Two or more computers connected together.

Network Manager: Someone who oversees the network, monitoring its performance, security, error detection and who implements access controls.

Offline: Term that implies that an item of hardware or software is no longer actively linked with the Internet. See Online below.

Online: Opposite of Offline - i.e. an item of hardware or software is actively linked with the Internet.

Operating System: The basic system that underpins computer operations and the foundation upon which all other programs operate. MSDOS, UNIX and
Windows are all examples of operating systems.

Plug-in: Small pieces of software that add to the capability of existing programs.

PDA: An acronym for personal digital assistant - a mobile device or palmtop computer.

POP: Acronym for Post Office Protocol or Point of Presence - the location where connections to a network or the Internet may be accessed via dial-up networking.

Remote Access: Accessing and/or processing data from a computer in a different location.

RGfL: Acronym for Rotherham Grid for Learning - provides fast, secure and effective broadband Internet and email access for Rotherham schools. At its heart is a network which also connects all the borough's schools together via a central point where both pupils and teaching staff can share resources.

Router: Mechanism for transferring data between one or more networks.

Server: Both the software and hardware that is used to provide access to an internet resource.

SIRO: Acronym for Senior Information Risk Owner - a senior manager who co-ordinates and takes responsibility for action related to e-security and eSafety.

SMTP: Acronym for Simple Mail Transport Protocol. The standard that governs how email is sent and received.

Software: The files, data and programs that allow a computer to function but have no physical dimensions. By way of contrast, see ‘Hardware’.

Terabyte: Unit for a vast amount of computer data, consisting of 1024 gigabytes.

Twitter: This is a free social networking and micro-blogging service that enables its users to send and read messages known as tweets. Tweets are text-based posts of up to 140 characters displayed on the author's profile page and delivered to the author's subscribers who are known as ‘followers’.

Upload: Send files to another computer, usually via FTP.

URL: Acronym for Universal Resource Locator otherwise known as the address of a website.

VoIP: Acronym for Voice over Internet Protocol - or using the internet to transmit voice conversations, a technique increasingly used within virtual classroom systems.

Virus: Self-replicating software that propagates itself from one computer system to another, normally devised with malicious or mischievous motives.

VLE: Acronym for Virtual Learning Environment (See Learning Platform).

VPN: Acronym for Virtual Private Network which is a software application to create a private computer link between computers in different locations.

Web space: Amount of data capacity available for the construction of web pages, normally measured in megabytes.

Website: Collection of linked web pages with a common theme, created for the same purpose.

World Wide Web: A global information resource made up of interconnected web pages.

Appendix **D**

(Glossary courtesy of Bedfordshire County Council)

Further Information and Guidance

The nature of eSafety and technology is evolving rapidly. You may wish to keep up to date with further information or advice which can be found from the following websites:

- www.parentscentre.gov.uk (Resource for parents)
- http://www.ceop.gov.uk/ (Child Exploitation and Online Protection Centre -Resources for schools, parents, children and young people and practitioners)
- www.iwf.org.uk (Internet Watch Foundation - reporting of illegal images or content)
- www.thinkuknow.co.uk (The Internet safety programme delivered by CEOP)
- www.netsmartzkids.org (Suitable for 5 – 17 year olds)
- http://www.kidzsmart.co.uk/index.html – (Suitable for all under children under 11 years)
- www.phonebrain.org.uk (Suitable for Years 5 – 8 year olds)
- www.bbc.co.uk/cbbc/help/safesurfing (Suitable for Years 3 and 4)
- www.hectorsworld.com (Suitable for Foundation Stage, Years 1 and 2 and is linked to the thinkuknow website above)
- www.teachernet.gov.uk (Resource for schools, LA's and other educational settings)
- www.digizen.org.uk (Materials from DfE around the issue of cyberbullying)
- www.becta.org.uk (Resource for the education sector and others including current model policies on eSafety)
- http://www.nextgenerationlearning.org.uk/ (Simple tips for parents / adults)
- http://www.rscb.org.uk/Home.aspx (Rotherham Safeguarding Children's Board – policies, procedures and practices.)
- http://www.nen.gov.uk/esafety (Resources for schools and other educational settings – including an online eSafety tool.)
- http://www.yhgfl.net/ (Yorkshire and Humber Grid for Learning – Consisting of a Regional Broadband Consortium)

- http://www.rotherham.gov.uk/info/442/librariescomputers_and_the_internet/601/computers_and_the_internet/2 (Rotherham Borough Council Libraries Service – Computers and the internet, on-line safety advice.)

- http://clickcleverclicksafe.direct.gov.uk/index.html (The UK Council for Child Internet Safety (UKCCIS) has launched a useful 'Click Clever, Click Safe Code designed to act as an everyday reminder of simple good behaviours, to help avoid common risks online)