St. John the Evangelist Catholic Academy

Part of the Newman Catholic Collegiate

Policy on Acceptable Use

Policy Written:	Date: March 2014
Ratified by the Academy Committee	Date: April 2015
Date for review:	Date: May 2018

St. John the Evangelist Catholic Academy

Acceptable Use Policy

Networked resources, including Internet access, are potentially available to students and staff in the academy. All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the academy. Any expression of a personal view about the academy or multi-academy company (MAC) matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the academy or multi-academy company (MAC) into disrepute is not allowed.

The academy expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources. *Independent pupil use of the Internet or the academy's Intranet will only be permitted upon receipt of signed permission and agreement forms as laid out below>*. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

CONDITIONS OF USE

Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to the Principal.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but the following list provides some guidelines on the matter:

NETWORK ETIQUETTE AND PRIVACY

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

1. Be polite – never send or encourage others to send abusive messages.
2. Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4. Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users files or folders.
5. Password – do not reveal your password to anyone. If you think someone has learned your password then contact *Mr Smith, ICT Subject Leader.*
6. Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
7. Disruptions – do not use the network in any way that would disrupt use of the network by others.
8. Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
9. Staff or students finding unsuitable websites through the school network should report the web address to the Head Teacher or Head of School.
10. Do not introduce "pen drives" into the network without having them checked for viruses.

11. Do not attempt to visit websites that might be considered inappropriate. (Such sites would include those relating to illegal activity, All sites visited leave evidence in the network if not on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.

12. Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.

13. Files held on the school's network will be regularly checked by *Mr Smith, Computing Leader.*

14.It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this

Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.

UNACCEPTABLE USE

Examples of unacceptable use include but are not limited to the following:

- Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.
- Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.
- *Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety.*
- *Accessing or creating, transmitting or publishing any defamatory material.*
- Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data.
- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.
- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

Additional guidelines

- Users must comply with the acceptable use policy of any other networks that they access.
- Users must not download software without approval from Mr Smith, ICT Co-ordinator.

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The academy will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are expected to inform Mr Smith, Computing Leader, immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

PHYSICAL SECURITY

Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used. Items that need to be left over breaks and lunchtimes for example will need to be physically protected by locks and or alarms.

WILFUL DAMAGE

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the academy system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

MEDIA PUBLICATIONS

Written permission from parents or carers will be obtained before photographs of pupils are published. Named images of pupils will only be published with the separate written consent of their parents or carers.

Publishing includes, but is not limited to:

- the academy website,
- the Local Authority web site,
- web broadcasting,
- TV presentations,
- Newspapers.

Pupils' work will only be published (e.g. photographs, videos, TV presentations, web pages etc) if parental consent has been given.

Staff Acceptable Use Agreement Form

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the academy's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Agreement Form.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies, relevant national and local guidance and expectations and the Law.

 I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops mobile phones, tablets, digital cameras, email and social media sites.

 Academy owned information systems must be used appropriately. I understand that 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.

 I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. 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 respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly).

 I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

 I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. 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, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by the use of encrypted memory stick. Any images or videos of pupils will only be used as stated in the photographic and filming policy and will always take into account parental consent.

- I will not keep or access professional documents which contain academy-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. Where possible I will use the academy's dropbox to upload any work documents and files in a password protected environment or via VPN. I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the academy computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

- I will respect copyright and intellectual property rights.

- I have read and understood the school online safety 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.

- I understand that mobile phones will not be used during lessons or formal school time and that the sending of abusive or inappropriate text messages is forbidden. The use of a mobile phone must be used in a suitable place.

- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead /e-Safety Coordinator (H. Buutters/L. Smith) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Mr. Smith as soon as possible.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any academy related documents or files, then I will report this to the ICT Support Team as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via academy approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships that may compromise this will be discussed with the Senior Leadership team and / or Principal.

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

- I will 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 school, or the County Council, into disrepute.

- I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead / online safety Coordinator (H. Butters/L. Smith).

- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

The Academy may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the Academy's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the academy will invoke its disciplinary procedure. If the academy suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: ………………………………………………………………………………………………

Print Name: ……………………………………………………………………………………… Date: ……………………..

Accepted by: ………………………………………………………………………………………….

Print Name: ……………………………………………………………………………………………