<u>All students, parents/guardians and staff members must read and agree to the below policy before the usage of any hardware, software or I.T. systems connected to the school.</u>

Draft I.T./Internet Acceptable Use Policy (IAUP)

John the Baptist Community School

1.1 Rationale for the policy

The following Internet Acceptable Use Policy or IAUP has been developed in accordance with the school's fundamental aim to foster in students a sense of self-reliance, independence, co-operation and responsibility and to provide them with skills for life-long learning where the school believes that access to the schools ICT resources plays an important role. It hopes to ensure that pupils will benefit from learning opportunities offered by the schools internet resources in a safe and effective manner.JTBCS' Acceptable Use Policy ("AUP") is also to prevent unauthorized access and other unlawful activities by users online. Internet use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP and the Code of Behaviour will be imposed.

As used in this policy, "user" includes anyone using the computers, Internet, email, chat rooms and other forms of direct electronic communications or equipment provided by JTBCS (the "network"). **Only current students or employees are authorized to use the network.** JTBCS reserves the right to monitor users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of JTBCS' property, network, and/or Internet access or files, including email.

Ratification and acceptance of this policy

Each school year, students must complete a signed page acknowledging this policy. Students who are under 18 must have their parents or guardians sign this page and schools must keep it on file. Once signed that permission/acknowledgement page remains in effect until revoked by the parent or the school. Teachers, students and other users are required to follow this policy. All users will be asked to also accept this policy when they attempt to logon to the school's internet and Moodle system for the first time. Even without a signature, all users must follow this policy and report any misuse of the network or Internet to a teacher, supervisor, or other appropriate JTBCS personnel. Access is provided primarily for education and JTBCS business. **By using the network, users have agreed to this policy.** If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a teacher, supervisor or other appropriate personnel.

This policy will be reviewed annually and submitted to the Board of Management of the school for ratification yearly after such regular reviews. The school and the Board of Management reserves the right to amend this policy throughout the year, as needs and issues arise that may need addressing within its remit.

IT Resources available:

- Two fully networked ICT Rooms with Broadband internet access for the use of teaching ICT. (Rooms 27/29)
- School Library with four computers with Broadband internet access.
- Every classroom has a desktop computer and data projector
- Staffroom has two computers with internet access
- Facility & Eportal software for school attendance and school reports available in all offices and staff computers.
- A number of laptops and portable Data Projectors are available to staff.
- Two interactive 98inch Promethean whiteboards (Room 15/25)
- Seven rooms equipped with ebeams
- The school Website is: www.johnthebaptistcs.ie

The following arrangements are presently in place for the provision of ICT education in the school:

- Leaving Certificate Applied have timetabled ICT classes – presentations and projects are a part of the programme and are assessed independently/externally.
- Leaving Certificate Vocational Programme have timetabled ICT classes. Presentations and projects are a key part of the programme and are assessed independently/externally.
- Other year groups may be brought to the ICT room by their respective subject teachers in pre-booked avaible class periods
- Supervised access to the internet is available in the school Library.

School's Strategy

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

Use of computer rooms

- Internet sessions will be supervised by a teacher.
- Each student will be assigned a specific computer to use whilst in the computer room as per the seating plan. Students may not use any other computer without the permission of the supervising teacher.
- Uploading and downloading of non-approved software, data files, image files, audio and video files will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of personal floppy disks, memory sticks, CD-ROMs, or other digital storage media in school requires a teacher's permission.
- Students will treat others with respect at all times and will not undertake any actions that may bring the school or its staff members into disrepute.
- Students will observe good etiquette i.e. etiquette on the internet at all times and will not undertake any actions that may bring the school into disrepute.
- Any use of the schools computing resources or Internet connection that could be considered bullying is in breach of this policy and in breach of the anti-bullying policy and will be treated accordingly.

Filtering Software/Censorship

Central to the debate on protecting children from inappropriate material on the Internet is the effectiveness of filtering software. Filtering is a term used to describe a way of limiting the content of web pages, emails, chat rooms and other electronic forums to which users may be exposed. Filtering software usually carries out the task of filtering. Filtering software operates using a set of criteria against which it judges whether Internet content is acceptable or not. For instance, the criteria could be a list of forbidden words, which the software seeks to identify on a web page or chat room. If the forbidden words are detected the filtering software blocks access to that location.

Although filtering software reduces the risk of accessing inappropriate material to some degree, it is only part of a wider strategy to promote online safety. Relying primarily on filtering software may place students in a position of greater vulnerability if the filtering software fails to function effectively. Filtering software enables the administrator to have some technical control over students' access to the Internet. Every effort will be made by JTBCS to ensure the viability and effective functioning of its filtering software. Fostering a culture of responsible use of the Internet is preferable and is in itself a valuable educational experience. It should be noted however, that given the dynamic nature of the wider internet environment along with limitations of technology and human endeavour that no guarantees can be provided in terms of being able to protect schools from all inappropriate or harmful content.

JTBCS will use technology protection measures to block or filter, to the extent practicable, access of visual depictions that *are obscene, pornographic, and harmful to minors* over the network. Filtering software and/or equivalent systems will be used in order to minimize the risk of exposure to inappropriate material. All unfiltered and possibly unregulated material/sites will be blocked on school computers as standard. This includes social networking and blogging mediums. Any attempt to access banned, unregulated or unsuitable sites will be reported to the IT coordinator. Such attempts will be met with a standardised webpage, informing the individual of what has occurred. In line with the school's policy, such an approach may lead to over blocking of sites. However, to ensure this does not adversely affect access to relevant, educational material, sites can be unblocked.

If a teacher wishes for a site to be unblocked on the school internet network, a submission must be made to the IT coordinator (see Appendices). It is advised that teachers who wish to make such a submission have checked/investigated the suggested site thoroughly for unsuitable material and links. The IT coordinator, management and the Board of Management reserve the right to refuse such a submission on the grounds that the suggested site may present an unacceptable risk or lead to harm of students or staff.

World Wide Web

Over half of 8-10 year old children in Ireland use the internet daily. This figure increases for those aged 10-16 years with over ¾ accessing the internet on a daily basis. Irish children's use of mobile phones and gaming consoles to access the internet is also above the European average with over 45% of children accessing the internet through such means (isfsi.ie). In the light of such statistics, mindful and careful use of the internet in school as well as the instilling in students of effective and safe guidelines for all internet usage is eesential.

- Students will not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will report accidental accessing of inappropriate material to the supervising teacher. The teacher must then record the incident in the Computer Room Record Book.
- Students will use the Internet for educational purposes only.
- Students will be made aware not to copy information into assignments and fail to acknowledge the source. This constitutes Plagiarism and Copyright Infringement.
- Students will be asked to never disclose or publicise personal information unless for educational purposes under the supervision of the teacher.
- Downloading and uploading materials or images not relevant to their studies is in direct breach of the schools acceptance use policy.
- Students will be made aware that any usage, including distributing or receiving information, school related or personal may be monitored for unusual activity, security and/or network management reasons.
- Much of the material available on filesharing sites is protected by copyright. Infringement of this copyright may lead to legal action being taken against people who upload or

download such materials and do not pay the appropriate charges levied by the owners. A significant number of cases have been taken by the music and film industry against individuals who have breached this copyright resulting in awards of thousands of euros against individuals, including children.

Internet Chat/Blogging/Online Gaming

- Students will only have access to chat rooms, discussion forums, messaging or other electronic communication forums for educational purposes and with the permission of the supervising teacher.
- Social networking sites including Bebo, MSN Messenger and any other similar sites are not allowed to be accessed.
- Students must not forget that the anonymous nature of chatrooms means that individuals can present themselves or their intentions in a manner that may not be honest or clear.
- If a situation or instance does not feel right or comfortable, students must report the situation to a teacher. Pupils are advised to keep copies of any materials involved.
- Proxy servers are strictly forbidden.
- Students will be encouraged where possible to use Usernames in order to avoid disclosures of identity.
- Face-to-face meetings with any third party organised via Internet chat are forbidden.
- Blogging can be a great way for you to share thoughts and opinions. However, its public nature means that students must take extreme care when posting to a blog (web log), even it is a personal blog. Personal information must not be revealed as blogs can be used to befriend students for questionable reasons, which may place pupils in danger.
- Posting inappropriate comments/pictures on blogs can be a particularly insidious form of cyberbullying. Students must take extreme care when posting.
- School hardware or software must not be used for gaming or games. Many such sites pose security and safety risks.

Browsing

The World Wide Web (www) can be considered a virtual library of information; as a result, many schools use it to find information published by other schools, governments, universities, companies and teacher organisations. One of the most compelling aspects of the World Wide Web is the ability to locate information by clicking on words or images – otherwise known as HTML (Hypertext Mark-up Language). This allows the user to navigate or browse web pages in a linear or non-linear fashion as they wish. In order to browse in this way an application known as a browser is required. The most popular browsers used are Internet Explorer and Firefox. Browsing can be hugely beneficial as it can allow exposure to a wide variety of educational material in multi-media formats and can develop the ability to broaden information research skills. However, students can equally be exposed to illegal, questionable, inauthentic or harmful material.

- **Guidelines for teachers (browsing)**

Teachers should:

- Preview or evaluate websites and internal links before providing student access. Alternatively, use an education web portal such as Scoilnet (www.scoilnet.ie) as a means of sourcing websites that have been previewed and approved by educators.
- Ensure online learning is directed and task-oriented. Consider the use of WebQuests or curriculumfocused websites such as TeachNet Ireland.
- Bookmark websites and encourage student to locate websites in this way.
- Consider offline browsing or the use of the virtual learning environment for controlled access to the Internet.
- Continuously monitor students' browsing activities by circulating in the room.
- Set time limits for Internet use to discourage aimless surfing.
- Keep a record of which students are allocated to each personal computer and how long they have been online. Every teacher must complete a seating plan for the computer room.
- Encourage any student who accidentally encounters illegal material to switch off their monitor immediately and report it to their teacher.
- Preview and select suitable websites before students begin their own searches.
- Test results of child-friendly search engines for the age appropriateness of content.
- Consider using search engines that have been designed for students with Internet safety in mind. These include:
    - http://www.askforkids.com/
    - http://yahooligans.yahoo.com/
    - http://www.education-world.com/
    - http://sunsite.berkeley.edu/KidsClick!/
- Teach students how to evaluate the content validity of websites (see form in Appendices)
- Ask students to ignore or close marketing banners that appear on certain websites.
- Remind students of any aspect of the school AUP and sanctions that relate to browsing the Internet.

Teachers and students are reminded that Google Safe Search is also an option. Google's SafeSearch screens for sites that contain explicit sexual content and deletes them from your search results. No filter is 100% accurate, but SafeSearch should eliminate most inappropriate material. SafeSearch settings can be changed on the Advanced Search or the Advanced Image Search pages on a per search basis. These pages can be accessed by clicking the Advanced Search link beside the search field in Google. You can choose from among three SafeSearch settings:

- Moderate filtering excludes most explicit images from Google Image Search results but doesn't filter ordinary websearch results. This is your default SafeSearch setting; receiving moderate filtering unless changed.

• Strict filtering applies SafeSearch filtering to all search results (i.e., both image search and ordinary web search).

• No Filtering.

Social Networking

Social networks have become a huge part of many individuals' lives in recent years e.g the huge increase in the usage of sites such as Facebook and microblogging sites such as Twitter. These sites are unfiltered and personal domains and therefore cannot be used in the school context.

Recent research has indicated that 75% of 13-14 year olds and 88% of 15-16 year olds have an online social networking profile. Although research states that over 60% of children in Ireland ensure their profiles are private, the number of "friends" children accept on social networking sites ranges from 200-1000+. Moreover a quarter of children aged 11-16 state they communicate online with people who they have never met in real life.

The use of social networks is forbidden within the school, using school hardware or software. Any efforts to access such sites will be automatically logged with the Internet filtering software and by extension the school's IT Coordinator.

Circulating, publishing or distributing (including on the internet) material associated with school activities, including but not limited to material in relation to staff and students which such circulation undermines, humilitates or causes damage to another person is considered a serioud breach of school discipline and may result in disciplinary action. As part of such disciplinary action, the Board of Management reserves the right to suspend or expel a student or students where it considers the actions to warrant such sanctions. In terms of usage outside the school environment, staff and students are encouraged to remember the following pointers:

- Privacy settings should be regularly reviewed and reset to ensure the level of provacy that one requires.
- No personal information such as home addresses or phone numbers should be made available on the site.
- Pictures posted on such sites become the property of such sites and therefore may be disseminated rapidly to a range of sources. Therefore, careful consideration must be taken when uploading any images. Students must remember that the information put on a profile can be seen by everybody. Once one places the information /photos on the Internet it can be seen and copied/used by others, i.e. one loses control over it, people may attempt to use it ways that students never intended.
- Updates/status updates can often, inadvertantly be viewed publically and may open an individual to anti-social behaviour.
- Students are reminded that individuals on such sites are not always what they seem; one cannot assume that the information supplied by other users on their profiles is authentic.

Students must take care when accepting people into chat areas and what is discussed in such areas.

- These sites can be used to carryout bullying and harassment. This is unacceptable and considered to be a breach of the school's anti-bullying policy. If this is the case, students are advised to:

✓ Save the evidence
✓ Don't respond in any shape or form to any provocation
✓ Tell an adult, teacher or someone that they trust

Cyberbullying

"Cyberbullying involves the use of information and communication technologies such as e-mail, cell phone and pager text messages, instant messaging (IM), defamatory personal Web sites, and defamatory online personal polling Web sites, to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others." –Bill Belsey (www.cyberbullying.org). This is a pervasive and completly unacceptable form of behavior and will not be accepted in the school.

Cyberbullying includes the following:

- Sending offensive, cruel or threatening messages, emails, photos or film
- Silent phone calls.
- Posting malicious comments or pictures on a bulletin board, website or chat room.
- Pretending to be someone else in a chat room or message board or text message and making malicious

  comments
- Accessing someone's accounts in order to scare them or cause trouble for them.

This list is not exhaustive and may continue to evolve.

Cyber-bullying is of great concern to John the Baptist Community School. If found to have occured, it is addressed using the mechanisms outlined in the Code of Behaviour and Bullying Policies of the school.

Email

Email or electronic mail has become a primary method of communication in recent years. Email is provided as part of JTBCS' overall provision of ICT facilities for the purpose of teaching, learning, and administration activities. JTBCS has the right to intercept access or review the contents of any email; electronic communication or files created and monitor usage on a random basis. This will be for the purposes of preventing, detecting or investigating crime or misuse, ascertaining compliance with regulatory standards and JTBCS policies, or to secure effective system operation.

JTBCS reserves the right to disclose the contents of any email or other electronic communications

to comply with or assist law enforcement officials or legal authorities.

Email: General

- Email is a communication tool and all users must use email in a responsible, effective and lawful manner. Email use is subject to relevant legislation.
- Students will not send or receive any material that is illegal, obscene, and/or defamatory or that is intended to annoy or intimidate another person.
- Students will not reveal their own or other peoples personal details, such as addresses or telephone numbers or pictures unless for educational purposes and under the supervision of the teacher.
- Students are asked to never arrange a face-to-face meeting with someone they only know through emails or the Internet.
- It can be possible that files shared through email or SPAM mail will often be misnamed to hide their actual content or even to entice people to open them. This is particularly true in relation to some types of pornographic material, especially child pornography. If students have any doubt about what a file may contain, it should not be opened and immediately deleted. Email can be used for the rapid spread of viruses and computer damaging sofware. Again, students must not open unknown or suspicious emails when they can not verify its source.

School Email

As part of the school's attempt to integrate and develop the use of IT for teaching and learning, the provision of a school email account for each student will commence in the academic year 2012/2013. This in turn leads requires further considerations:

- Students will be asked to use a school email address where necessary and not personal email accounts. Students will use these approved email accounts in class under supervision by or with permission from a teacher.
- Authorised users are issued with an email account with the domain name "johnthebaptistcs.ie". Therefore, when using the school email, all users are reminded that they are representing the school. Thus, all users must ensure that they must not act or use the account in a way that would bring the school, other students or staff into disrepute.
- This account should be secured by the user with a personal password.
- An e-mail account may only be used by the person to whom it is assigned and is not to be shared with anyone for any reason. The account and password should be protected accordingly to prevent abuse. The owner of the account will be held responsible for any illegal activity that occurs from the use of the account.
- Users should not use the school email as the basis of signing up to external websites or activities. This would open the account to possible nefarious material and software. This is to be avoided at all costs.
- In some circumstances legitimate access may be allowed to another persons' email

accounts e.g. Secretary, Head of Year and this will be in the event of long term absence due to serious illness or annual leave. Such access to a Users account in these instances must be approved by the Head Teacher, Deputy Head Teacher or Network Manager. Every user is responsible for ensuring that appropriate arrangements are made to cover periods of absence.

- Individuals are permitted to reveal IT passwords to the Network Manager and/or authorised IT Technicians where required for problem resolution or administration purposes.
- Any misuse of the account will be an offence and may be liable to prosecution.
- Users are reminded that this is a school email and therefore should only be used for school purposes.
- Students will note that sending and receiving email attachments using the approved school email account is subject to extreme caution.
- Students must inform a teacher or IT cooordinator if their account becomes subject to unsolicitated email/SPAM or becomes inadvertently involved in unsuitable actiivities.

- **Email Account closure**

When a member of staff leaves the employment of JTBCS, their email account is cancelled. Likewise, student email accounts are closed after the cessation of their studies at the school.

User Accounts can also be closed under the following conditions:

- Staff email accounts remain open for a discretionary period, usually one calendar month after a staff member has left.
- Staff should ensure that they unsubscribe from any email lists that they have subscribed to and delete any personal emails in their account. If there are any work related emails that need transferring to another user, then these emails should be forwarded on as appropriate.
- Student email accounts are closed after the cessation of studies with a grace period of one calendar month from the last day of the final term of study.
- Where leavers have a need to retain links with the school, email accounts can be kept open beyond the one calendar month up to a maximum period of three calendar months if required. The decision to extend the discretionary period must be authorized by the relevant senior member of staff/Board of Management and advised to the Network Manager.
- If a member of staff is dismissed from employment due to misconduct or dies whilst in employment – the account is immediately closed. Any data stored under their account can be released upon appropriate liaison between JTBCS and the relevant Head of School / Network Manager to other individuals under normal legal safeguards as required.
- JTBCS reserves the right to redirect / allow access to the email accounts for legitimate purposes of those staff that have left during the one month calendar period.

- **All email users must be mindful and may become liable in the following areas:**
  - **Intellectual Property :** Anyone who uses email to send or retrieve any materials that infringe the intellectual property rights of a third party may be liable to that third party if such use is not authorised by them
  - **Obscenity:** A criminal offence is committed if a person publishes any material which is pornographic, excessively violent. It is an offence to publish or distribute obscene material of a child.
  - **Defamation**: As a form of publication, the Internet is within the scope of legislation relating to libel where a statement or opinion is published which adversely affects the reputation of a person, group of people or an organisation. Legal responsibility for the transmission of any defamatory, obscene or rude remarks which discredit an identifiable individual or organisation will rest mainly with the sender of the email and may lead to substantial financial penalties being imposed.
  - **Data Protection:** Processing information including photographs which contains personal data about individuals requires the express written consent of those individuals. Any use of personal data beyond that registered with the Information Commissioner will be considered illegal.
  - **Copyright**: Users must be mindful of copyright issues in relation to creations, including text, graphics and sounds by an author or an artist. This will include any which are accessible through JTBCS ICT facilities. Any uploading or downloading of information through on-line technologies which is not authorised by the copyright owner will be deemed to be an infringement of their rights.
  - **Discrimination:** Any material disseminated which is discriminatory or encourages discrimination may be unlawful where it involves discrimination on the grounds of sex, sexual orientation, religion, race or disability

School Website

The school website is a vital part of the internet/cyber presence of the school and is a valuable tool in terms of public realtions and information desimination for parents, teachers, students and other relevant parties. However, the public nature of the medium means that particular effort and precautions must be taken in relation to its presentation and implementation.

- The website will be regularly checked by senior staff to ensure that there is no content that compromises the safety of pupils or staff.
- The publication of students work will be coordinated by a teacher and subject to the approval of senior management.
- Pupils work will appear in an educational context on web pages with a copyright notice prohibiting the copying of such work without express written permission.
- The school will endeavour to use digital photographs video and audio clips focusing on group activities. Content focusing on individual students will not be published on the school website without parental approval.

- Personal pupil and staff information including home address and contact details will be omitted from school web pages.
- The school website will avoid publishing the surname of any student in a photograph.
- The school will ensure that the image files are appropriately named – will not use pupil's names in image file names or ALT tags if published on the web.
- Class lists will never be printed on the website.
- Photographs of children will focus on the activity they are engaged in.
- A student's name will not be printed beside their photograph.
- Pupils will continue to own the copyright on any of their work published on the school website.
- All materials used in the school website will be reviewed under the school's Data Protection Policy.

Virtual Learning Environment

A Virtual Learning Environment (VLE) is a specilaised closed web-based interface that assists learning and teaching through providing and integrating online resources and tools. It has become very popular among educators around the world as a tool for creating online dynamic web sites for their students.

The school currently utilises Moodle (Modular Object-Oriented Dynamic Learning Environment). Moodle is a Course Management System (CMS), also known as a Learning Management System (LMS). It is a Free web application that educators can use to create effective online learning sites in a controoled, restricted manner.

Since all pupils seek to use ICT to enhance their learning across the curriculum, the Virtual Learning Environment (VLE) has been developed to provide a wide range of interactive activities, course support materials and access to supported structures of learning in a safe and monitored online environment. School staff will be responsible for the development, upgrading and updating of course contents, taking appropriate steps to ensure that materials for the use on the VLE are in addition to and do not replace those available in the classroom.

The VLE provides opportunities for online communication and access to a range of course materials, offered in different formats e.g. video, audio, text, use of graphics etc. It also hosts wikis, blogs and quiz tools. Communication facilities include Instant Messaging (IM), discussion forums, web conferencing, virtual meetings and email.

Staff/specialised staff are happy to give parents advice if they have any concerns about the home use of computers for accessing any course information, discussion forums, chat facilities, school email or messaging facilities hosted in the VLE.

Aim of VLE/Moodle

- Allows pupils to access an online learning structure specifically designed to enhance their learning experiences

- Facilitates the acquisition of transferable ICT skills that can be used in other curriculum areas in school, in continuing education or training and in employment
- Encourages pupils to engage in valuable collaborative learning experiences and receive online mentoring support from peers and teachers
- Provides invaluable developmental, enhancement and enrichment opportunities for students and teachers

Please Note:

- All VLE users should be aware that comments made through the communication facilities may reflect not only on themselves but also on JTBCS as an organisation. Individuals' use of the VLE's communication facilities should only have a positive impact on the reputation of JTBCS.
- Contributions through and to the communication fora, blogs and wikis are regarded as the intellectual property of the authors. If contributions are to be quoted by another guidance counsellor in an assignment, acknowledgment must be given.
- Every teacher will have the opportunity to gain the necessary knowledge to monitor every pupil's use of this medium. Teachers have the necessary pedagogical knowledge to devise appropriate courses for use on the VLE and will be given the technical support to transfer information into a web-based format by the Webmaster.
- The school provides a filtered and monitored access to the VLE for pupils and staff. Nonetheless, no filtering service can be completely foolproof, and teachers ensure that pupils using the VLE from school behave in a responsible manner.
- Pupils and staff are made aware that the school routinely tracks and records discussion forums and chat facilities within the VLE
- Pupils are aware that written communications on the VLE are monitored by teachers. While normal privacy is respected and protected by password controls, users must be aware that written communications stored on the VLE are not absolutely and unconditionally private.

Security

- The VLE has been designed to offer safe and secure access to activities and materials deemed suitable by teachers/school, without the possible nefarious impact of external forces. Therefore, any attempt to open the VLE to outside influences will be treated severely.
- Each individual is responsible for the security of any usernames and passwords they are issued with. Pupils and Staff must not disclose their usernames and passwords to anyone .
- Students are advised that the once issued with a user name and password that both cannot be changed, except by the VLE administrator. This is a difficult process and can take a long period. Therefore, students must keep both pieces safe.
- If a problem occurs with loggimng or either password/usernames, users are advised to

inform the administrator as soon as possible.

Students Must Not:

- Use the VLE in such a way that disrupts the use of the VLE by other users
- Download software or other files without permission.
- Send inappropriate e-mails, messages or engage in inappropriate, abusive or defamatory chat and forums
- Publish, share or distribute any personal information about any user (such as: home address; email address; phone number; photos)
- Use another user's password or allow other users to use their password
- Communicate to others any information, or engage in any activity which may result in the loss of or damage to another pupil's work
- Retrieve, send, copy or display offensive or pornographic information or images
- Use obscene, discriminatory or racist language, harass, insult or attack others
- Upload or use malicious code in any form within the VLE
- Search out or use security threats as this may constitute an illegal attempt to gain access to the VLE
- Disrespect other people's opinions and beliefs.
- Do anything to endanger the anonymity of third parties (e.g. colleagues, students etc.) where requested and appropriate.

Viruses and Malare protection

Computer viruses are items of software that attach themselves to other legitimate items of software or data, without the consent of the computer user, and are programmed to proliferate themselves onto other computers, often to cause disruption or damage. It is essential that all users play a part in protecting the network from the presence of viruses.

The school has obtained a school wide licence for anti-virus to combat computer viruses and other forms of malare such as trojans and worms. It is the policy of the school to run up to date virus protection software on all computers that are attached to the network. This software will automatically report the presence of most known viruses. Any user who receives an on-screen warning from this software (these are very clear and explicit) should stop all use of the computer immediately and report the occurrence to the present teacher or ICT coordinator. The teacher in turn should report this event to the IT coordinator. Viruses can attach themselves easily to removable storage media and this is one of the main ways in which they proliferate. The software used to prevent students from tampering with various computer settings will also, to some extent, prevent them from accessing these removable media. However this is not totally secure.

Furthermore, there are instances in which students and staff will want to transfer data to and from the network on removable media, e.g. as a means of submitting homework/projects or to work on materials in school and at home. To allow for this and still ensure system security it is the school's policy that all removable mediamust be virus scanned before being accessed through any

computer on the network. These must be re-scanned again each time they are used in computer outside the network. Please give reasonable notice to system administrators if scanning is needed.

Thus, to ensure virus security and control, it is essential that:

- No hardware is connected to the school network without downloading/subscribing to the school's antivirus
- All USBs/portable data modules are scanned by the school anti-virus before opening using school hardware

Eportal

ePortal is a powerful web-based interface that allows access to relevant data from a central source, through secure, password-protected entry. Teachers can reach accurate facts about students immediately, learners can track their own performance and parents can check their children's progress. This AUP applies whenever access to John the Baptist Community School's ePortal management system interface is provided. This policy applies whenever information is accessed through ePortal, whether the computer equipment used is owned by this school or not. The policy applies to all those who may make use of the ePortal Service, including but not limited to, all members of staff employed in JTBCS either in a permanent or temporary basis, all parents or guardians of pupils attending the school and any other persons to whom ePortal access may from time to time be granted. Password-protection means that the system can identify users and restrict access to authorised areas. Eportal can be accessed in school or at home. Links are also available of the school website under the "Teacher" section.

Features and Benefits:

- Easy access from any internet connection
- Information is quickly and easily available to all who need it
- Simple interface for easy data input
- Improves communications between teachers, students and parents

This policy section is intended to minimise security risks. These risks might affect the integrity of JTBCS' data, the Authorised ePortal User and the individuals to which the ePortal data pertains. In particular these risks arise from:

- The intentional or unintentional disclosure of login credentials to the ePortal system by authorised users;
- The wrongful disclosure of private, sensitive, and confidential information;
- Exposure of JTBCS to vicarious liability for information wrongfully disclosed by authorised users.

JTBCS' ePortal system is provided for use only by persons who are legally responsible for pupil(s) currently attending the school. Information made available through the ePortal system is confidential and protected by law under the Data Protection Act 1988. Access is granted only on condition that the individual formally agrees to the terms of this Policy.The authorising member(s) of school staff must confirm that there is a legitimate entitlement to access information for pupils

the names of whom must be stated on the ePortal Parental Access

JTBCS reserves the right to revoke or deny access to the ePortal system of any individual under the following circumstances:

- The validity of parental responsibility is questioned
- Court ruling preventing access to child or family members is issued
- Users found to be in breach of the ePortal usage policy
- If any child protection concerns are raised or disputes occur the school will revoke access
- for all parties concerned pending investigation.
- Users are liable for any potential misuse of the system and/or breach of the data protection act that
- may occur as a result of failing to adhere to any of the rules/guidelines listed in this document

Users of ePortal agree to:

- Not share their username or password with any third parties,
- Use the system only as designated in this policy
- Do nothing with, and inform the school immediately, should they have access to data that is not specific to their child.
- ensure all relevant aspects of the Data Protection Act (1988) and the Freedom of Information Act (1997) are adhered to.
- ensure that the data is correct and to notify the School of any errors/changes in circumstance
- not distribute or disclose any information obtained from the ePortal system to any person(s) with the exception of the pupil to which the information relates or to other adults with parental responsibility;
- not attempt to access the ePortal system in any environment where the security of the information contained in the ePortal system may be placed at risk e.g. a cybercafé
- assume personal responsibility for your username and password and never use anyone else's username or password. Individual usernames and passwords must be kept confidential.
- These usernames and passwords should never be disclosed to third parties.
- Passwords will be assigned by the school.
- Lost or forgotten login details may be retrieved by contacting the IT coordinator.

Please note:

- The School reserves the right to examine or delete files or comments that may be held on its computer system.
- Please note that the School monitors ePortal and School Web Site access.
- Activity that threatens the integrity of the School ICT systems or activity that attacks or corrupts other systems is forbidden.

- Copyright of all materials must be respected.
  Intentional misuse of the ePortal system may result in ePortal
  users should address any complaints and enquiries about the ePortal system to JTBCS by email: or by telephone at .

Password Policy

- Personal responsibility is expected username and password.
- Passwords should be kept confidential. It is unacceptable to use another's password. Passwords and user names should never be shared.
- Users are advised not to use passwords for multiple online uses.
- Passwords used in the school must have the following:
  - ✓ Passwords must be at least 6 characters (a-z, 0-9) in length
  - ✓ Passwords must contain at least 1 number / symbol
  - ✓ Passwords must contain a mix of upper and lowercase letters
  - ✓ Passwords must not be similar to your own name or username for example: Cutler1

Personal Devices

Pupils using their own technology in school such as leaving a mobile turned on or using it in class, sending nuisance text messages, or the unauthorised taking of images with a mobile phone camera still or moving is in direct breach of the schools acceptable use policy and of the school's mobile phone policy and will be dealt with accordingly. Please refer to the School's Mobile Phone Policy for more details.

Other personal devices such as PSPs,Ipods/MP3/MP4 players, electronic tablets etc. are currently not allowed to be used in the school. Please note that some form of devices such as electronoc readers e.g. Kindles, Sony eReaders, Kobos etc. may be used in class and in the library under the strict supervision of staff and teachers. Only material approved by teachers may be read using such devices. The use of such devices is at the descretion of the teacher.

Legislation

There is no specific legislation governing Internet safety at school level. This is complicated by the fact that the Internet functions in a global context whereas the law functions in a localised one. The following pieces of legislation however have relevance to Internet safety and staff and students should be mindful of below:

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998: This Act legislates against any one who knowingly produces, prints, publishes, distributes, exports, imports, shows, possesses or sells child pornography.
- The Interception of Postal Packets and Telecommunications Messages Regulation Act, 1993: This Act stipulates that telecommunication messages can be intercepted for the

purpose of an investigation of a serious offence.

- Video Recordings Act 1989: This prohibits the distribution of videos which contain obscene or indecent material which may lead to the depravation or corruption of the viewer.
- The Data Protection Act 1988: This Act was passed to deal with privacy issues arising from the increasing amount of information kept on computer about individuals.

Roles and Responsibilities – Teachers

- Teachers will assign specific places in the computer rooms and where necessary, approved school email accounts to each student in each class.
- Teachers will closely supervise students use of computers at all times.
- Teachers will explain and revisit the AUP in September and in January of each academic year.
- Teachers will ensure that students Internet use will be planned, task-orientated and educational within a regulated and managed environment.

Roles and Responsibilities – Students

The following are unacceptable usages of school hardware, software or the school network.

- Violating any state or international laws such as: Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information, or copyrighted materials;
- Criminal activities that can be punished under law;
- Deliberate attempt to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any school computer system.
- Selling or purchasing illegal items or substances;
- Spamming; spreading viruses;
- Causing harm to others or damage to their property, such as:
  - Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others, or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
  - Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity,
  - impersonating other users, or sending email anonymously;
  - Damaging computer equipment, files, data, or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
- Using any JTBCS computer to pursue "hacking," internal or external to JTBCS or attempting to access information protected by privacy laws; or
- Accessing, transmitting, or downloading large files, including copyrighted media, chain letters or any type of pyramid schemes.
- Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:
  - Using another's account password(s) or identifier(s);
  - Interfering with other users' ability to access their account(s); or

- Disclosing anyone's password to others or allowing them to use another's account(s)
- Using the network or Internet for commercial purposes:
- Using the Internet for personal advertising, promotion, or financial gain; or conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes or lobbying for personal political purposes.

JTBCS reserves the right to take immediate action regarding activities that
(1) create security and/or safety issues for students, employees, schools, network, or computer resources, or
(2) that expend JTBCS resources on content JTBCS in its sole discretion determines lacks legitimate educational content/purpose, or
(3) other activities as determined by JTBCS as inappropriate.

Penalties for Improper Use

The use of a JTBCS account is a privilege, not a right, and misuse will result in the restriction or cancellation of the account. Misuse may also lead to disciplinary and/or legal action for both students and employees, including suspension, expulsion, dismissal from JTBCS employment, or criminal prosecution by government authorities. JTBCS will attempt to tailor any disciplinary action to the specific issues related to each violation in accordance with the school Code of Behaviour. The school also reserves the right to report any illegal activities to the appropriate authorities.

Disclaimer

JTBCS makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of JTBCS' network are to be borne by the user. JTBCS also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of JTBCS, its affiliates, or employees.

Some websites with more information and guidelines:

(as suggested by Dr. Maureen Griffin, Forensic Psychologist)

- ✓ Internet Safety for Schools Ireland http://www.isfsi.ie
- ✓ Office for Internet Safety –provides resources, explanations of technology, publications and tips www.internetsafety.ie
- ✓ Web wise –provides parents, teachers and children with educational resources, advice and information about potential dangers on-line www.webwise.ie

- ✓ Watch Your Space –provides advice on managing children's profiles on social-networking sites www.watchyourspace.ie
- ✓ Sexting Acronyms –provides an explanation of net lingo http://www.netlingo.com/acronyms.php
- ✓ Urban Dictionary –provides an explanation of everyday slang used by children http://www.urbandictionary.com/
- ✓ 02 –offers information on child protection services available www.02.ie/childprotection
- ✓ That's Not Cool website which offers tips and advice for both parents and children re: mobile phones & texting www.ThatsNotCool.com
- ✓ Common Sense Media -provides resources, advice and information for parents and children on a range of technological issues www.commonsense.org
- ✓ Mobile Minder http://www.mobileminder.com
- ✓ A Parent's Guide to Facebook www.connectsafely.org/pdfs/fbparents.pdf
- ✓ A Parent's Guide to Mobile Phones www.ispai.ie/docs/mobgd08.pdf
- ✓ Xbox 360 console parental controls http://support.xbox.com/en-IE/billing-and-subscriptions/parental-controls/xbox-live-parental-control
- ✓ Safer Search Engines for Children
- http://www.askforkids.com/
- http://yahooligans.yahoo.com/
- http://www.education-world.com/

ANNUAL REVIEW

The aim of this Acceptable Use Policy is to ensure that all users will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. It is envisaged that school and parent representatives will revise the AUP annually.

This version of the AUP was created on: _____ and was ratified by the Board of Management of John the Baptist Community School on: _____

Signed: _____ _____

ICT Coordinator Principal

AUP checklist

For an AUP to be robust it needs to be reviewed and updated regularly taking into consideration implementation issues that may arise. The following is a checklist that may be used when revising the school's AUP.

- ☑ Have AUP implementation issues arisen since the AUP was designed/revised? All issues that arise between pre-planned revision dates should be noted on the attached sheet.
- ☑ Have these issues been discussed with parents, students and teachers and incorporated into an updated AUP?
- ☑ Given that an AUP is in place, can the school confidently address the following scenarios?

- ☑ A student is found using a chat room to arrange a face-to-face meeting with a friend
- ☑ The school uses filtering software but a student accidentally accesses a pornographic website while in your care
- ☑ A student publishes defamatory information on a personal website about a peer
- ☑ Has the AUP had a positive impact on curriculum delivery?
- ☑ Has internal or external expertise assisted the formulation or reformulation of the AUP?
- ☑ Has the AUP as a code of Internet use transferred to home use?
- ☑ Does an open dialogue exist between students and teachers relating to Internet misuse and safety issues?
- ☑ Are teachers' and students' internet safety training needs being met