St John Fisher Catholic Voluntary Academy

E-Safety policy

Approved November 2017
Review date: November 2018

Academy's Mission Committee

Contents

The Blessed Peter Snow Catholic Academy Trust

The Catholic Voluntary Academies which form the Blessed Peter Snow Catholic Academy Trust are distinctive as we provide grounding in the Catholic Faith for all our children. The special character of our Catholic academies is the quality of the religious teaching, integrated into the overall education of our children. Our beliefs, which are Gospel centred, affect the way we live, making our academies living examples of Christ and His teachings.

"Education is not and must never be considered as purely utilitarian. It is about forming the human person, equipping him or her to live life to the full – in short it is about imparting wisdom. And true wisdom is inseparable from knowledge of the Creator.'" (Pope Benedict XVI, Address to Teachers and Religious, Twickenham, September 2010).

Our Academies therefore operate and are informed by the following four key principles of Christian formation:

- **Places of Discipleship**
- **Places where Communities are created**
- **Places of Learning**
- **Places where we treasure God's World**

In light of the above principles, the Trust aims to:

- ensure secure, welcoming and engaging environments in which all individuals learn to value and respect both themselves and others
- provide all individuals with the opportunities to achieve excellence, to develop their full potential as human beings and to encourage and challenge them to do so
- uphold the unshakable belief in the unique potential of each child, student and member of staff
- provide a curriculum that initiates students into the knowledge, values, attitudes and skills they need to become mature Christian adults in their personal, social, family and working lives.

Mission Statement

Following the example of our patron, St John Fisher, priest and scholar, we aim to love one another throughout our life at school, to learn and develop our full potential in the image of Christ.

1. Background

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and Academy Councillors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (Positive behaviour, Anti-bullying and Safeguarding and Child Protection).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to

manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2. Scope of the policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

3. Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school

Academy Councillors:
Academy Councillors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. A member of the Academy Council has taken on the role of E-Safety Academy Councillor. The role of the E-Safety Academy Councillor will include:

- *regular meetings with the E-Safety Officer*
- *regular monitoring of e-safety incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Academy Councils committee / meeting*

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Officer
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the

internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Headteacher and Designated Senior Leader for safeguarding and child protection should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Officer:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with school ICT technical staff
- receives reports of e-safety incidents
- meets regularly with E-Safety Academy Councillor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings / committees of Academy Councils

Network Manager / Technical staff:

The Network Manager / Technical staff are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Filtering Policy Template" for good practice document)
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Officer / Headteacher
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and annually signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Officer / Headteacher

- digital communications with students (email / Virtual Learning Environment / Twitter) should be on a professional level and only carried out using official school systems - please see attached appendix on use of Twitter specifically
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students understand and follow the school e-safety and acceptable use policy
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Senior Leader for Safeguarding and Child Protection:
The DSL (Clare Kernan) and the Deputy DSL (Kate Lea) should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students:

- are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy (in Planners), which they will be expected to sign before being given access to school systems. Passwords must be kept secure and secret
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Additionally, all students in Year 7 will complete an accredited level 1 e-safety course as part of their ICT curriculum.

Parents / Carers:
Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that

many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through an annual parents' information evening for Year 7, and updates via the school website. They should also:

- ensure their child has read, understood and signed the Student Acceptable Use Policy in Planners, and signed it themselves
    - Sign the letter included in the New Entrants pack regarding safe use of ICT
    - access the school website / VLE / Schools information management system (SIMS) in accordance with the relevant school Acceptable Use Policy
    - monitor their child's use of the Internet at home including social network sites such as Facebook

4. Educating all users

Education of students:

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme is taught as part of ICT / PSHCE. This will cover both the use of ICT and new technologies in school and outside school. Year 7 will complete an accredited level 1 e-safety programme
- Key e-safety messages will be reinforced as part of a planned programme of assemblies
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be helped to understand the need for the student Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the interne
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- Rules for safe Internet usage are included in all student planners

Education of parents / carers:

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through

- The school website
- A Year 7 parents information evening

Education of staff:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Officer will receive regular updates through attendance at relevant training courses
- The E-Safety Officer will provide advice / guidance / training as required to individuals as required

Education of Academy Councillors:

The named E-Safety Academy Councillor should take part in e-safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Academy Councils Association
- Participation in school training / information sessions for staff or parents

5. Technical – infrastructure / equipment / filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets e-safety technical requirements
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager
- All users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames.
- The "administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and kept in a secure place. A school should never allow one user to have sole administrator access.
- Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must

immediately report any suspicion or evidence that there has been a breach of security.

- The school maintains and supports the managed filtering service provided by the local authority
- The school has provided enhanced user-level filtering through the use of the Smoothwall filtering programme.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to the ICT Network Manager.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager. If the request is agreed, this action will be recorded.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy
- Remote management tools are used by staff to control workstations and view user activity
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager or E-Safety Officer. This is by direct email to the address ict@stjohnfisher.org.uk. This will be publicised on the school website for all users
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- There is provision for the temporary access of "guests" (eg trainee teachers, visitors) onto the school system through a Guest Account. Supply staff also have access through a Supply Account. Passwords are changed regularly.
- The downloading of executable files is barred in school. On school laptops staff should only download school related files.
- Laptops provided by school can be used for limited personal use by the member of staff only. They should be password secured and stored safely at all times.
- The school infrastructure and individual workstations are protected by up to date virus software. Memory devices are virus checked through the school system / laptops when installed.
- Student data should only be taken out of school on a secure laptop or memory device which is password protected.

6. Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum:

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes

are in place for dealing with any unsuitable material that is found in internet searches.

- Where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

7. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow the school policy concerning the sharing, distribution and publication of those images. **Those images should only be taken on school equipment.**

The personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of students are published on the school website
- Student's work can only be published with the permission of the student and parents or carers.

8. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

Staff must ensure that they:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The device must be password protected
- The device must be checked for viruses using school anti-virus software
- The data must be securely deleted from the device, once it has been transferred or its use is complete

This is in conjunction with the new General Data Protection Regulation which comes into force May 2018.

9. Communication

Mobile phones:

Students may bring a mobile phone to school but it must be switched off between the hours of 8.55 am and 3.20 pm and out of sight. It is to be used for journeys to and from school only. Staff should not use their own personal phones in the classroom and must take calls etc in their own time. Phones should always be on silent in the classroom. Staff should never use their own personal phones to take images of children, nor should they ever give their own personal phone numbers to students.

Email:
Staff and students may only use school email addresses for communication. Personal email addresses should never be used. Communication must be professional in tone and content. The official school email service may be regarded as safe and secure and is monitored. Users must immediately report, to the E-Safety Officer, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

10. Banned user actions

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on any materials, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images
- The promotion or conduct of illegal acts
- Adult material (which is likely to breach the Obscene Publications Act)
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Threatening behaviour including promotion of physical violence or mental harm
- Any other information which may be offensive or breaches the integrity of the ethos of the school or brings the school into disrepute
- On line gaming
- On line gambling
- On line shopping (for anything other than school purposes)
- Use of social networking sites other than the school Twitter account

11. Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal disciplinary procedures unless it is judged that illegal activity has taken place in which case the police and local authority will need to be involved.

Appendix 1

Twitter guidelines for St John Fisher staff

The use of Twitter by teachers can be of great benefit to staff, students and parents if used correctly and effectively as an aid to support teaching and learning. The immediacy and accessibility of Twitter means it can be an effective tool to:

- Communicate information about school events to parents and students.
- Showcase the learning activities that take place in school, letting parents and the wider community see what's happening in our community.
- Allow teachers to share interesting, relevant educational material online with students and to set work or reminders.
- Allow staff to share good practice and work collaboratively.

It is important that Twitter is used effectively and also safely, for the welfare of both staff and students. In order to ensure that safe and effective use is maintained, please follow these guidelines if you use Twitter for school purposes:

- Staff must set up a separate professional account and must only use this account to communicate with students or to make tweets that are school related. This must be the only account that is used to communicate to students
- In order to maintain uniformity so that it's easy for students and parents to follow teachers, try to incorporate the school Twitter address which is @sjfdewsbury, and your own initials
  For example: for Joe Bloggs use the address: @jbsjfdewsbury
- Ensure that a relevant professional photograph and biography is attached to the account if including one
- When setting up the account, ensure that you select 'Private tweets' to ensure that your tweets are only viewed by those who follow you. However, anyone can choose to follow you so professional conduct must be maintained at all times
- Once a professional account is set up, inform students of the address to follow and inform line managers and the Headteacher's PA of the address so that a directory of Twitter accounts can be kept and viewed on staffshare
- To ensure that content remains one way and transparent, do not follow the students who follow you – no 'Direct Messaging' should take place between staff and students
- Only school related content to be used – no personal information or personal comments/opinions to be tweeted from the professional account
- Check photo consent before broadcasting any images of students
- Include @sjfdewsbury in your tweet if it is relevant to the wider community – these may then be re-tweeted
- Ensure that information for students via Twitter is accessible by other means too, to ensure fair access for all students

SLT line managers must follow staff professional accounts to ensure that content is relevant and to maintain the welfare of staff and students.

These guidelines have been provided in the interests of staff and students to ensure that Twitter is used safely and effectively. Failure to follow the guidelines when using Twitter could be deemed as professional misconduct and lead to subsequent disciplinary action.

Appendix 2
ICT Acceptable Use

Staff and Student Acceptable Usage Policy (AUP)
This simplified code of conduct applies at all times, either in and out of school hours, whilst using school equipment. Please read it carefully.

Users
All users must respect all equipment.
You may be billed for equipment damage, including labour fees.
Please make I.C.T Staff aware immediately of any virus warning or threat.
Respect copyright and trademarks (material cannot be copied without giving credit to the person or company that owns it.).

I.C.T Suites and facilities

Students must:
- always seek staff permission before using a computer
- not use the Curriculum computers outside lesson times, unless been supervised by a member of Staff
- monitor their user space and keep it below the limit. This is currently set to 500mb for the 6th form and 100mb for the rest of the school
- read & agree to the Internet Acceptable Use Policy before using the Internet
- read & agree to any other Acceptable Use Policies as appropriate
- read & agree to any local rules such as those posted on the walls of the classroom

Please Note: Unsupervised students sent to I.C.T Suites will be refused entry.

When using an I.C.T Suite Teaching Staff have a duty to ensure:
- Faults or requests are reported either during or after a lesson.
- Students do not move the equipment (PCs, printers, printer cartridges, keyboards or mice) from their positions – this often leads to damage.
- Ensure rooms are left tidy - any paper left strewn about will be thrown away. Belongings will be kept for 2 weeks then either sent to lost property or disposed of.
- Switch off overhead projectors after use. The bulbs for these are £300+ and we have had cases of them left on over the holiday periods.

All users (Staff and Students) must not:
- Use anyone else's logon account.
- Use the Network (or save files) for any other purpose which is not directly related to School work.
- Run any program not officially installed on the network, regardless of why it is needed.
- Attempt to install any computer programme.
- Software requests must go via the I.C.T Manager – a minimum of 2 weeks notice must be given for any software installations (appropriate licenses must be acquired.)
- Save files with either offensive content or filenames. (Such files will be deleted regardless of content).
- File names over 255 characters will be periodically deleted.

- Send, access or display offensive messages or pictures.
- Attempt to hack, modify or infect the network using any code, programme or virus.
- Attempt to circumvent security policies.
- Use or send bad language in documents.
- Intentionally waste resources thus preventing use by others.
- Eat or drink near any machine, or in any computer room.
- Play games or engage in other non curricular activities.

Please note: All files placed in your Curriculum/Admin User area, Shared areas and emails will be treated as School property. Your log on and log off records will automatically be kept by the system. All Internet activity is logged and periodically checked. We use this information to check that inappropriate sites are not accessed and to take action to ensure Students and Staff cannot view such material.

User areas on the school network are closely monitored and I.C.T Support may review files and communications to maintain system integrity and the law. We may discreetly monitor your screen using software. The two main reasons for this are to monitor misuse of the system and to remotely assist you should a problem arise.
You will not be made aware when we are connected to your computer, however only authorised Staff have access to this monitoring software.

We have remote control software installed in I.C.T Suites, Offices and Faculty Rooms which allows the teacher (in I.C.T Suites) to monitor and take control of students' machines, and also allows I.C.T Support to monitor and fix problems remotely.

Should a user be found misusing the system, we may gather evidence against them from our logs and monitoring software to prove they are involved in the incident. This information may be used against them in matters where they have broken one or more Acceptable Usage Policies and/or the relevant law.

Main I.C.T Responsibilities AUP (Also Available in the Staff Handbook)

- The school requires all users to comply with the provisions and obligations of all legislation and with the conditions of use imposed by the various funding authorities which relate to the use of I.C.T, for example: The Data Protection Act, 1998; the Copyright, Designs and Patents Act 1988, and other European Union directives; the Computer Misuse Act 1990; The Freedom of Information Act 2000; and the Joint Academic Network (JANET) Acceptable Use Policy, which is issued by UKERNA (the UK Education and Research Networking Association). All users must also comply with the policies, regulations and guidelines for the use of I.C.T issued from time to time by the Headteacher.
- Hacking and the deliberate introduction of viruses into any I.C.T system are serious offences and are subject to the School's disciplinary regulations.
- Any use of I.C.T resources, for example email or Internet, which is illegal, indecent, offensive, threatening, which harasses any person, whether a member of the School or not, or which may constitute a criminal offence is forbidden and may be subject to the School's disciplinary regulations.
- The I.C.T resources provided by the School are intended for use in relation to the work, or in the interest of the School. Limited personal use is permitted provided it does not interfere with the work of others or jeopardise the interests of the School.

- I.C.T resources provided by the School may not be used for commercial activity, for advertising or for fundraising, except for School-related activities, unless such activities have been specifically approved by the Headteacher. A charge may be levied for such use.
- Users are expected to comply with the School's Acceptable Use Policies for I.C.T Facilities issued from time to time by the Headteacher, e.g. use shall not be made by any individual of any username or identity or I.C.T resources allocated to another person, unless such use has been specifically authorised by the owner, or the Headteacher.
- Similarly, an individual may not give any other person use of any username, or identity, or I.C.T resource which has been allocated to them, unless such use has been specifically authorised by the Headteacher.
- No one shall wilfully or deliberately jeopardise the integrity of the equipment, facilities, programs, or other stored information, or other person's work, or invade another person's privacy.
- The copying, modification, dissemination or destruction of software, programmes or any similar proprietary information or other action that may constitute a criminal offence is forbidden.
- Breaching the access or security of any I.C.T systems, wherever based, is forbidden. Searching for security loopholes is considered as serious as actually breaching security.
- Users are not permitted to exploit commercial programs, results, or other material developed using School I.C.T resources, unless such exploitation has been specifically authorised by the Headteacher.
- Connection of equipment to the School Network is only permitted with the permission of the Technical Manager. Personal laptops or similar devices (whether connected directly or via wireless link) must be registered with I.C.T Technical Support (Technical Manager) before connection. Wireless base stations may only be connected if configured by a member of the I.C.T Technical Support team.

AUP for Internet and Email usage.

- The school reserves the right to examine or delete any files that may be held on its computer system and to monitor any Internet sites visited and emails exchanged.
- Users are not allowed to use schools computers for any form of illegal activity. e.g. downloading copyright materials, introducing viruses, hacking into other computers.
- The sending of racially abusive or other offensive email using school facilities is considered a criminal act.
- Viewing, storing, transferring or downloading pornographic, obscene, offensive or any other inappropriate material from any source is forbidden.
- Carrying out personal financial transactions (e.g. using sites such as eBay, a credit or debit card; internet banking) is strongly discouraged for staff and forbidden for students.
- Anyone accessing unacceptable material by accident should immediately inform I.C.T Support.
- Newsgroups will only be for educational purposes.
- Do not post anonymous messages or forward chain letters.
- Users are responsible for all email sent and received, including from newsgroups, and must be vigilant about the risk of virus infection from files attached to emails.
- You should never provide the school email address for personal use.

- School email will not be used for sending private or personal messages.
- Users must not wilfully make any changes to computer settings, delete any software or interfere with another persons work files.
- Users will not use schools computers to play Internet games.
- The use of chat lines is forbidden unless specifically set up as an educational chat room.

You must check that material brought in from home is virus free.

Student Misuse of the Internet/Network
Students found to be abusing the facilities will have either their account disabled or access to the Internet removed. Internet access will be re-instated after the matter has been resolved with the student and/or the student's teacher. Please note: restoring access to the internet is seen as a very low priority job and may not be done immediately.

Three abuses of trust will lead to accounts being permanently disabled – and a solution must be agreed with teachers, heads of year and perhaps senior team. All students should be referred to helpdesk or the I.C.T Support office for account related issues.

Please Note: Internet Access will NOT be enabled on an Ad Hoc (Lesson to Lesson) Basis.

E-mail Policy
Your email will not be read on a random or casual basis unless we have reason to believe you are acting in an unreasonable manner. All emails are automatically spam and virus checked as they are sent through our mail server. We reserve the right to automatically check for and flag up offensive material. Email attachments which contain more than one full stop [.] will be automatically quarantined and not sent or received. Incoming and outgoing email that contains swearwords or characters that may be of an offensive nature will also be quarantined. Occasionally mistakes are made with the filtering – for example an email that ends "love and kisses xxx" would be quarantined because the characters "xxx" also denote hardcore pornography. Please let I.C.T Support know if you feel an incoming or outgoing email has gone astray.

User Areas, Print Usage and Adhering to AUPs
Your disk and printer usage will be audited on a regular basis to ensure that correct levels have been set.

Failure to follow relevant Acceptable Use Policies may result in loss of access and further disciplinary action may be taken if appropriate. All parties (you and us) are obliged to act within the law and abide by any Local Authority Policies regarding computer use. If applicable, external agencies may be involved as certain activities may constitute a criminal offence.

We reserve the right to amend these rules at any time and changes will be made on the Logon Acceptable Use Policy and Intranet Community Section. These rules apply to Student & Staff use of both the Curriculum and Administration Networks.

Equality Impact Assessment

School	**St John Fisher Catholic Voluntary Academy**
Date	**November 2017**
Lead member of staff	**C Kernan**
Other involved staff/role	**M Ward / A Kerrison**

Proposed Plan

Background/ how this proposal has come about

Reason for proposal – to introduce new practice/provision
to change or reduce practice/provision
to remove practice/provision

Main stakeholders

Any legislation or guidance that informs the proposals

Introduction of an E-Safety policy for the school covering all aspects of staff, student and parent use of ICT Updated November 2017

Is the proposal likely to have an adverse impact on compliance with the Equality Duty?

Eliminating unlawful discrimination, harassment and victimisation Y/**N**
Promoting equality of opportunity Y/**N**
Fostering good relations Y**/N**
Please explain

Consultation Process
With whom do you plan to consult?
How?
Where is the evidence of the consultation?

Potential Issues

Characteristic	**Impact of proposal (specify if impact is to pupil, parent/carer, staff,** academy councillor**, other)**	**Positive Negative Neutral**	**Can barrier be removed? Y/N**
Disability		**Neutral**	
Race		**Neutral**	
Sex		**Neutral**	
Gender reassignment		**Neutral**	
Pregnancy, maternity		**Neutral**	
Religion/belief		**Neutral**	
Sexual orientation		**Neutral**	
Marriage, civil partnership		**Neutral**	
Age		**Neutral**	

Explain in more detail
